CAROTENUTO
STUDIO LEGALE

The Client Update

Newsletter no. 3 (Year 4) – June 2022

Periodic newsletter prepared by *Carotenuto Studio Legale* on the main EU and Italian law and case-law novelties.

L'Informazione al Cliente

Lettera informativa n. 3 (Anno IV) – Giugno 2022

Lettera informativa periodica di Carotenuto Studio Legale sulle principali novità normative e giurisprudenziali europee ed italiane.

Table of contents - Indice

Top stories	In primo piano
Annual Report of BoI's Governor	**Relazione del Governatore della BdI**
On 31 May 2022, BoI published its annual report, from which it appears that:	Il 31 maggio 2022 la BdI ha pubblicato la relazione annuale, dalla quale si evince che:

a) international economy, thanks to the vaccination campaigns, is recovering with an increase in demand. Nevertheless, the war in Ukraine has led to a sharp deterioration in growth expectations accompanied by a rise in commodity prices;
b) persistent supply bottlenecks of energy goods weakened economic activity in the latter part of the year, however, in almost all euro area countries, deficits and debt have declined from their extremely high levels in 2020;
c) Italian economy improved strongly in 2021, GDP increased by 6.6 %. Growth occurred in all Italian regions with excellent results. Household income grew as a result of increased employment and public interventions to combat the pandemic;
d) in the area of public finance, there was a significant improvement in public accounts. General government net borrowing fell to 7.2%.

In his final remarks to the Report, BoI's Governor issued a hopeful warning to the RRF, which "*will be able to contribute to the strengthening and expansion of the most dynamic segments of our production system, as well as of the financial industry*".

BoI's Annual Report 2021, published on the official website on 31 May 2022

a) l'economia internazionale, grazie alle campagne vaccinali, sta recuperando con un aumento della domanda. Tuttavia, la guerra in Ucraina ha determinato un peggioramento delle aspettative di crescita accompagnate da un rincaro dei prezzi delle materie prime;
b) le difficoltà di approvvigionamento dei beni energetici hanno indebolito l'attività economica alla fine dell'anno, tuttavia, in quasi tutti i paesi dell'area dell'euro, il disavanzo e il debito sono diminuiti rispetto al 2020;
c) l'economia italiana nel 2021 ha registrato un miglioramento, il PIL è aumentato del 6,6%. La crescita è avvenuta in tutte le regioni italiane con ottimi risultati. Il reddito delle famiglie è cresciuto grazie all'aumento dell'occupazione e agli interventi pubblici;
d) nell'ambito della finanza pubblica si è registrato un significativo miglioramento dei conti pubblici. L'indebitamento netto delle amministrazioni pubbliche è sceso al 7,2%.

Nelle considerazioni finali alla Relazione, il Governatore ha lanciato un monito di speranza nei confronti del PNRR che "*potrà contribuire al rafforzamento e all'espansione dei segmenti più dinamici del nostro sistema produttivo, nonché dell'industria finanziaria*".

Relazione annuale 2021 della BdI, pubblicata sul sito ufficiale il 31 maggio 2022

Register of beneficial ownership

A Decree has been recently issued by MEF, jointly with MED, which provides for the communication of data and information on the beneficial ownership of companies with legal personality, private legal persons, trusts and similar institutions.

Notification of beneficial ownership must be made to the territorially competent register of companies by:

a) directors of companies having legal personality;
b) founder, if alive, or persons entrusted with the representation and administration of private legal persons;
c) trustee of trusts or similar institutions.

In addition, the above mentioned persons are required to notify:

a) any changes in the beneficial ownership within 30 days therefrom; and
b) confirmation of the above data and information within 12 months from the first or latest notification and then annually.

Finally, please note that the obligation to file the afore-side communications must be satisfied within 60 days of the entry into force of the Decree on 9 June 2022.

MEF and MED's Decree of 11 March 2022 no. 55, (published in the Official Gazette on 25 May 2022 no. 121)

Registro del titolare effettivo

È stato recentemente pubblicato il decreto del MEF di concerto con il MiSE, che disciplina la comunicazione dei dati e delle informazioni relativi alla titolarità effettiva di imprese dotate di personalità giuridica, persone giuridiche private, trust e istituti affini.

I soggetti che devono comunicare al registro delle imprese territorialmente competente la titolarità effettiva sono:

a) gli amministratori delle imprese dotate di personalità giuridica;
b) il fondatore, se in vita, o i soggetti cui è attribuita la rappresentanza e l'amministrazione delle persone giuridiche private;
c) il fiduciario di trust o di istituti affini.

Inoltre, gli stessi sono tenuti a comunicare:

a) eventuali variazioni della titolarità effettiva entro 30 giorni dalla variazione; e
b) la conferma dei dati e delle informazioni entro 12 mesi dalla prima comunicazione o da quella di variazione e poi annualmente.

I suddetti obblighi devono essere adempiuti entro 60 giorni dall'entrata in vigore del presente decreto, prevista per il prossimo 9 giugno.

Decreto del MEF di concerto con il Mise del 11 marzo 2022 n. 55, (pubblicato in G.U. il 25 maggio 2022 n. 121)

Ukraine-*bis* Decree

On 21 May 2022 entered into force a Decree laying down urgent measures to counter the economic and humanitarian effects deriving from the invasion of Ukraine by the Russian Federation.

Among the main novelties, the modification of the regulation of the so-called "golden power" (i.e., the Government's special powers to safeguard the ownership structure and management of national companies operating in strategic and national interest sectors).

In particular, the establishment of new companies of strategic importance for defence and national security is subject to a notification requirement. Moreover, in the communication, energy, transport, health, agribusiness and finance sectors, the afore-said notification requirement is extended to the purchase of significant shareholdings made by European entities (including those resident in Italy), to the extent to which it determines the permanent establishment in Italy of the company at issue on the ground of the change of control over the latter.

In order to strengthen the coordination activities leading to the exercise of the golden power, a strategic evaluation and analysis working group has been established within the Department for administrative coordination at the Presidency of the Council of Ministers.

Decreto Ucraina-*bis*

Il 21 maggio è entrato in vigore il decreto che prevede misure urgenti per contrastare gli effetti economici e umanitari derivanti dall'invasione dell'Ucraina da parte della Russia.

Tra gli interventi più rilevanti, è stata modificata la disciplina dei c.d. "*golden power*", (ovvero dei poteri speciali del Governo, funzionali alla salvaguardia degli assetti proprietari e della gestione di società nazionali operanti in settori strategici e di interesse nazionale).

In particolare, la costituzione di nuova impresa di rilevanza strategica per la difesa e sicurezza nazionale è soggetta all'obbligo di notifica. Inoltre, nei settori delle comunicazioni, energia, trasporti, salute, agroalimentare e finanziario, tale obbligo di notifica viene esteso agli acquisti di partecipazioni rilevanti compiuti da soggetti europei (anche residenti in Italia), nella misura in cui l'acquisto determini l'insediamento stabile in ragione dell'assunzione del controllo della società.

Al fine di potenziare l'attività di coordinamento delle attività propedeutiche all'esercizio dei *golden power*, è stato istituito un nucleo di valutazione e analisi strategica, presso il dipartimento per il coordinamento amministrativo della Presidenza del Consiglio dei ministri.

Law of 20 May 2022 no. 51, converting Law Decree of 21 March 2022 no. 21 (published in the Official Gazette on 20 May 2022 no. 117)

National Cybersecurity Strategy

A national cybersecurity authority has been established by means of Law Decree no. 82/2021, for the purpose of protecting national interests in the cyberspace.

In addition, a national cybersecurity strategy for the years 2022-2026 has been defined, which aims at planning, coordinating and implementing measures to make Italy a more secure and resilient country from the risks associated with the digital transition. Among such risks, it is worth mentioning:

a) cyber attacks, which exploit software errors, misconfigurations and weaknesses in protocols in order to steal data or damage the IT systems; and
b) the spread of fake news, deep-fakes and disinformation campaigns, which tend to confuse and destabilise citizens through cyberspace.

In order to accomplish the afore-said goals (namely, protection of national strategic assets, response to cyber threats, secure development of technologies), the following enabling factors are deemed indispensable:

a) training (i.e., creating a solid national workforce of experts and young talents with the necessary skills and competences); and

Legge n. 51 del 20 maggio 2022, di conversione del D.L. 21 marzo 2022, n. 21 (pubblicato in Gazzetta Ufficiale il 20 maggio 2022 n. 117)

Strategia nazionale di cybersicurezza

L'agenzia nazionale per la cybersicurezza, è stata istituita con il D.L. n. 82/2021, a tutela degli interessi nazionali nel cyberspazio.

Inoltre, la strategia nazionale di cybersicurezza, per gli anni 2022-2026, è stata adottata al fine di pianificare, coordinare e attuare misure tese a rendere l'Italia un paese più sicuro e resiliente dai rischi connessi alla transizione digitale. Tra questi rischi, si annoverano:

a) attacchi *cyber* che sfruttano errori *software*, errate configurazioni, debolezze nei protocolli per sottrarre dati o arrecare danni ai sistemi; e
b) diffusione, attraverso lo spazio cibernetico, di *fake news*, *deep-fake* e campagne di disinformazione che tendono a confondere e destabilizzare i cittadini.

Per poter realizzare gli obiettivi (protezione degli *asset* strategici nazionali, risposta alle minacce e alle crisi cyber, sviluppo consapevole e sicuro delle tecnologie), sono indispensabili i seguenti fattori abilitanti:

a) la formazione (ovvero, creare una solida forza lavoro nazionale, composta da esperti e giovani talenti in possesso delle capacità e delle competenze necessarie); e

b) promoting a cyber security culture, raising awareness in the public and private sectors and, in particular, in the civil society about cyber risks and threats (including cyber bullying that, although not new, never ceases to create social alarm). *National Cyber Security Strategy 2022-2026, Council of Ministers Presidential Decree of 17 May 2022 (published on the Official Gazette on 1 June 2022 no. 127)*	b) promuovere la cultura della sicurezza cibernetica, aumentare la consapevolezza nel settore pubblico e privato ed in particolare nella società civile sui rischi e le minacce *cyber* (tra le quali il fenomeno del cyber bullismo, che, ancorché non nuovo, non cessa di creare allarme sociale). *Strategia nazionale di cybersicurezza 2022-2026, adottata con decreto del Presidente del Consiglio dei ministri il 17 maggio 2022 (pubblicata in Gazzetta Ufficiale l'1 giugno 2022 n. 127)*

Corporate/ Laws of contract	Diritto societario/Contrattualistica

On the "russian roulette clause": the Supreme Court delves into its validity

In view of the absolute novelty and complexity of the issues raised in the proceedings in question, the Court of Cassation has recently entrusted its office of maxims with the task to carry out an in-depth analysis of the legislative, case-law and doctrinal framework (including United States and Canada) of the regulation of the anti-waiver clause known as "russian roulette clause", focusing in particular on its validity and effectiveness among the parties to a given contract.

Supreme Court, Civil Section I, Interlocutory Order no. 13545 of 29 April 2022

Clausola "*russian roulette*": la Cassazione vuole approfondirne la validità

Con ordinanza, la Corte di Cassazione, in relazione all'assoluta novità e complessità delle questioni sollevate nel corso del giudizio, ha affidato all'ufficio del Massimario un approfondimento, del quadro normativo, giurisprudenziale e dottrinale, anche statunitense e canadese, relativo alla disciplina della clausola antistallo denominata "*russian roulette clause*", con particolare riguardo alla sua validità ed efficacia tra le parti stipulanti.

Cassazione civile, I sezione, ordinanza interlocutoria del 29 aprile 2022 n. 13545

Banking law	Diritto bancario

Online fraud: limits of the bank's liability

The Criminal Court of Parma has recently rejected an appeal against a fraud allegedly made online. The appellant had also sued the bank in question in order to obtain the return of the sums allegedly stolen.

On the merits, the court has ascertained that the bank cannot be held liable on the ground of the appellant's negligent behaviour in respect of using such means of payment

Indeed, pursuant to Article 12 of Legislative Decree no. 11/2010, all losses arising from unauthorized payment transactions are attributable to the client who acted fraudulently or failed to fulfill obligations concerning the use of the payment means envisaged under the contract entered into with the bank.

Therefore, in the case at issue the client had violated his contractual obligations, as in the days prior to the disallowed payments he had provided his personal and non-transferable access data to an unknown person during a phone call (followed by many others). In addition, the client had failed to notify the bank of the afore-said situation.

On the same topic, the Supreme Court has recently held liable a bank for lack of debtor's

Truffa *online*: i limiti di responsabilità della banca

Il Tribunale penale di Parma ha recentemente respinto un ricorso contro una presunta truffa online. Il ricorrente aveva citato in giudizio la banca in questione per ottenere la restituzione delle somme asseritamente sottratte.

Nel merito, il tribunale ha accertato che la banca non può essere ritenuta responsabile per il comportamento negligente del ricorrente nell'utilizzo di tali mezzi di pagamento.

Infatti, ai sensi dell'art. 12 del D. Lgs. 11/2010, tutte le perdite derivanti da operazioni di pagamento non autorizzate sono imputabili al cliente che ha agito in modo fraudolento o non ha adempiuto agli obblighi relativi all'utilizzo dei mezzi di pagamento previsti dal contratto stipulato con la banca.

Pertanto, nel caso in questione il cliente aveva violato i suoi obblighi contrattuali, poiché nei giorni precedenti ai pagamenti non autorizzati aveva fornito i suoi dati di accesso personali e non trasferibili a una persona sconosciuta durante una telefonata (seguita da molte altre). Inoltre, il cliente non aveva comunicato alla banca la suddetta situazione.

Sullo stesso tema, la Corte di Cassazione ha recentemente ritenuto responsabile una banca per mancanza di diligenza del debitore

diligence in fulfilling the contract, since it had not adopted suitable means to counter unauthorised access to its clients' home banking system. In fact, according to the bank's professional diligence principle – whereby the bank must comply with the parameters of the so-called "prudent banker" – adequate means of proving a transaction must be put in place, capable of tracing back the client who has carried out such transaction. In the case decided by the Cassation, while the client had correctly alleged the bank's failure to act (i.e., to counteract the unlawful withdrawal), the bank failed to prove to have been compliant with the prudential rules governing the use of the home banking system.

Criminal Court of Parma, order of 27 April 2022 and Supreme Court, Civil section I, decision of 20 May 2022 no. 16417

The Board of Auditors' duty of control over internal bodies with administrative functions

In the corporate structure of banks, the system of internal controls does not limit the control obligations and duties of the board of auditors. In fact, persons in charge of internal control activities have a support function of the board of auditors, but do not replace the latter in its task.

nell'adempimento del contratto, in quanto non aveva adottato strumenti idonei a contrastare l'accesso non autorizzato al sistema di *home banking* dei propri clienti. Infatti, in base al principio di diligenza professionale della banca - che prevede il rispetto dei parametri del cosiddetto "banchiere prudente" - è necessario predisporre adeguati strumenti di prova di un'operazione, in grado di risalire al cliente che l'ha effettuata. Nel caso deciso dalla Cassazione, se da un lato il cliente aveva correttamente denunciato l'omissione della banca (cioè di contrastare il prelievo illegittimo), dall'altro la banca non ha dimostrato di aver rispettato le norme prudenziali che regolano l'utilizzo del sistema di *home banking*.

Tribunale penale di Parma, ordinanza del 27 aprile 2022 e Cassazione Civile, sez. I, sentenza del 20 maggio 2022 n. 16417

Il dovere di controllo del collegio sindacale sugli organi interni con funzioni amministrative

Nella struttura societaria delle banche, la presenza di un sistema di controlli interni non limita gli obblighi e i doveri di controllo che incombono sul collegio sindacale. Infatti, i soggetti preposti ad attività di controllo interno hanno una funzione di supporto al collegio sindacale, ma non si sostituiscono a questo nella sua funzione di controllo.

The board of auditors is, in any case, required to ensure constant supervision of the work of the persons entrusted with administrative and management functions, with the obligation to verify the correctness, both formal and substantive, of the procedures and processes implemented, monitoring any dysfunctions, anomalies or deficiencies.

Supreme Court, civil section II, decision of 19 May 2022, no. 16276

EBA's report on shadow banking system

EBA published its final proposal of regulatory technical standards that set out the criteria for identifying shadow banking entities for the purposes of supervisory reporting on large exposures. Entities that perform banking activities or services, authorised and supervised, in accordance with EU law, are not shadow-banking entities.

Similarly, entities established in a third country that are authorised and monitored by a supervisory authority that applies the Basel core principles (for effective banking supervision) or that are subject to a regulatory regime recognised as equivalent to that applied in EU are not shadow-banking entities.

EBA Final Report, Draft regulatory technical standards on criteria for the identification of shadow banking entities pursuant to Article 394, paragraph 4, of Regulation no 575/2013/EU of 23 May 2022

Il collegio sindacale è, in ogni caso, tenuto ad assicurare una costante sorveglianza sull'operato dei soggetti incaricati di funzioni amministrative e gestionali, con l'obbligo di riscontrare la correttezza, formale e sostanziale, delle procedure e dei processi messi in atto, monitorando eventuali disfunzioni, anomalie o carenze.

Cassazione civile, sez. II, sentenza del 19 maggio 2022, n.16276

Relazione dell'ABE sul sistema bancario ombra

L'ABE ha pubblicato la proposta finale di norme tecniche di regolamentazione che stabiliscono i criteri per identificare i soggetti del sistema bancario ombra ai fini delle segnalazioni di vigilanza riguardanti le grandi esposizioni. Le entità che svolgono attività o servizi bancari, autorizzate e sottoposte a vigilanza, conformemente alla normativa euro-comunitaria, non sono entità bancarie ombra.

Altresì, non sono entità bancarie ombra, gli enti stabiliti in un Paese terzo, autorizzati e vigilati da un'autorità di vigilanza che applica i principi fondamentali di Basilea (per un'efficace vigilanza bancaria) o che sono soggette a un regime regolamentare riconosciuto come equivalente a quello applicato nell'UE.

Relazione finale dell'ABE, Progetto di standard tecnici di regolamentazione sui criteri di identificazione delle entità del sistema bancario ombra ai sensi dell'articolo

394, comma 4, del Regolamento n. 575/2013/UE del 23 maggio 2022

Financial law	Diritto finanziario

ESMA report on best execution reporting

ESMA has published a report to the European Commission on best execution supervisory reporting for investment firms under the MiFID II, in order to ensure an effective and consistent level of regulation and supervision and to enhance investor protection.

Best execution is the obligation for intermediaries, when executing client orders, to take appropriate and effective steps to achieve the best possible result for clients, with regard to price, cost, speed of execution and type of order.

In particular, ESMA suggests to:

a) improve the quality of supervisory reporting by removing the requirement for firms to report on the characteristics of executed orders, as this has not proven effective under the current regulatory framework
b) facilitate the use of reporting arrangements.

Final Report, "Review of the MiFID II regulatory framework on best execution reporting by investment firms", published on ESMA website on 16 May 2022

Relazione dell'ESMA sulle segnalazioni di *best execution*

L'ESMA ha pubblicato una relazione rivolta alla Commissione europea in materia di segnalazioni di vigilanza per le imprese di investimento sulla *best execution* ai sensi della MiFID II, al fine di assicurare un livello efficace di regolamentazione e vigilanza e per migliorare la protezione degli investitori.

La *best execution* è l'obbligo per gli intermediari, nell'esecuzione degli ordini dei clienti, di adottare misure adeguate per conseguire il miglior risultato possibile per la clientela, in riferimento al prezzo, costi, rapidità di esecuzione e tipo di ordine.

In particolare, l'ESMA suggerisce di:

a) migliorare la qualità delle informazioni relative alle segnalazioni di vigilanza, eliminando l'obbligo di segnalazione per le imprese sulle caratteristiche degli ordini eseguiti, in quanto non si è dimostrato efficace nell'ambito dell'attuale quadro normativo;
b) facilitare l'utilizzo delle modalità di segnalazione.

Relazione finale, "Revisione del quadro normativo MiFID II sulle segnalazioni di best execution da parte

delle imprese di investimento", pubblicata sul sito dell'ESMA il 16 maggio 2022

How to prove the assignment of receivables

Court of Appeal of Ancona, in accordance with other case law, has held that the proof of the title of credit must be provided by means of the assignment contract, from which it is clearly and unequivocally inferred that the disputed credit has actually been assigned.

In accordance with the Court, the publication of the assignment's notice in the Official Gazette is not sufficient to prove the title of the credit, but it only gives notice of the assignment, without providing for the specific indication of the assigned receivables.

Court of Appeal of Ancona, decision of 3 May 2022

Come si prova la cessione di crediti

La Corte d'appello di Ancona, in conformità con altre pronunce giurisprudenziali, ha affermato che la prova della titolarità del credito deve essere fornita attraverso il contratto di cessione, da cui si ricavi in modo chiaro ed univoco che il credito oggetto di contestazione è stato effettivamente ceduto.

Secondo la Corte, la pubblicazione dell'avviso di cessione nella Gazzetta Ufficiale non è sufficiente a provare la titolarità del credito, bensì dà solo notizia dell'avvenuta cessione, senza prevedere la specifica indicazione dei crediti ceduti.

Corte d'appello di Ancona, sentenza del 3 maggio 2022

Compliance | Conformità alle norme

Legislative Decree no. 231/2001 | *D.Lgs. n. 231/2001*

The absence of the organisational model does not automatically determine the administrative liability of the entity

La mancata adozione di un modello organizzativo non determina automaticamente la responsabilità amministrativa dell'ente

The fourth section of the Supreme Court distinguished the legal entity's liability from that of the senior officers, perpetrators of the crime.

The Court ruled that the absence or the ineffective implementation of the organisational and management models (Articles 6 and 7 of Decree 231 and Article 30 of Legislative Decree no. 81/2008) do not rise *ex se* to the constituent elements of the entity's offence. On the contrary, it is necessary to prove organisational fault (i.e. a set of measures capable of preventing the commission of offences of the type committed), by the Prosecutor, whereas the entity may prove the absence of such fault.

With regard to the liability of senior officers, the Court has found them liable for omissions and violations of preventive regulations; however, such conduct does not automatically result in the liability of the entity.

Supreme Court, criminal section IV, decision of 10 May 2022 no. 18413

La quarta sezione della Corte di Cassazione ha distinto il profilo di responsabilità dell'ente da quello dei soggetti apicali, autori del reato.

La Corte ha stabilito che la mancata adozione o l'inefficace attuazione dei modelli di organizzazione e di gestione (Artt. 6 e 7 del Decreto 231 e art. 30 del d.lgs. n. 81/2008) non assurgono *ex se* ad elementi costitutivi dell'illecito dell'ente. È invece necessario dimostrare la colpa di organizzazione (ovvero un insieme di accorgimenti preventivi idonei ad evitare la commissione di reati del tipo di quello realizzato) da parte dell'accusa, mentre l'ente può dare dimostrazione dell'assenza di tale colpa.

Sotto il profilo della responsabilità dei soggetti apicali, la Corte li ha riconosciuto responsabili per omissioni e violazioni della normativa prevenzionistica; tuttavia, tali condotte non determinano l'automatica responsabilità dell'ente.

Cassazione penale, sez. IV, sentenza del 10 maggio 2022 n. 18413

Data protection | *Protezione dei dati personali*

Protecting the whistleblower's privacy

Whistleblowing is a corporate compliance tool through which employees or third parties of a company can report, in a confidential and protected manner, any wrongdoing encountered in the course of their work.

Il *whistleblowing* deve tutelare la *privacy* del segnalante

Il *whistleblowing* è uno strumento di *compliance* aziendale, tramite il quale i dipendenti oppure terze parti di un'azienda possono segnalare, in

Recently, DPA sanctioned a hospital and the IT companies that operated whistleblowing service for violating the regulations under the GDPR. The companies used systems that recorded and stored users' browsing data, allowing them to be identified, including potential whistleblowers.

In particular, the healthcare company had not informed workers in advance about the processing of personal data carried out for the purpose of reporting wrongdoing, had not conducted a privacy impact assessment, and had not even entered such operations into the register of processing activities (a useful tool for assessing risks to the rights and freedoms of data subjects).

Privacy Guarantor's provision no. 134 of 7 April 2022

"Uber" penalty of more than €4 million

DPA has sanctioned Uber B.V, headquartered in Amsterdam, and Uber Technologies Inc, headquartered in San Francisco, for a total of € 4 million and 240,000.

The fines were applied following inspections conducted at Uber Italy Ltd. in connection with a data breach reported by the U.S. parent company in 2017. Companies were sanctioned as joint data controllers, each responsible for

modo riservato e protetto, eventuali illeciti riscontrati durante la propria attività.

Recentemente, il Garante privacy ha sanzionato un'azienda ospedaliera e la società informatica che gestiva il servizio di *whistleblowing* per aver violato il GDPR. Le società utilizzavano sistemi che registravano e conservavano i dati di navigazione degli utenti, consentendo l'identificazione degli stessi, tra cui i potenziali segnalanti.

Nello specifico, la struttura sanitaria non aveva informato preventivamente i lavoratori in merito al trattamento dei dati personali effettuato per finalità di segnalazione degli illeciti, non aveva effettuato una valutazione di impatto *privacy* e non aveva neppure inserito tali operazioni nel registro delle attività di trattamento (uno strumento utile per valutare i rischi per i diritti e le libertà degli interessati).

Provvedimento del Garante Privacy n. 134 del 7 aprile 2022

"Uber" sanzionata per più di 4 milioni di euro

Il Garante Privacy ha sanzionato Uber B.V, con sede legale ad Amsterdam, e *Uber Technologies Inc*, con sede legale a San Francisco per 4 milioni e 240.000 euro complessivi.

Le sanzioni sono state applicate in seguito ad accertamenti ispettivi effettuati presso Uber Italy s.r.l in occasione di un *data breach* segnalato dalla capogruppo statunitense nel 2017. Le società sono state sanzionate, come contitolari

violations of privacy law committed against Italian users, about 1.5 million, including drivers and passengers.

The penalties concerned:

a) the unsuitability of the information given to users, without the indication of co-ownership of the processing, generic and approximate with unclear and incomplete information. Processing's purposes were not specified, references to the rights of data subjects were vague and incomplete, and it was unclear whether or not users were obliged to provide their data;
b) lack of valid consent to data processing; and
c) lack of notification to DPA of data processing for geolocation purposes.

DPA's provision no. 101 of 24 March 2022

del trattamento, ciascuna responsabile per le violazioni della normativa *privacy* commesse nei confronti degli utenti italiani, circa 1 milione e mezzo, tra autisti e passeggeri.

Le sanzioni riguardavano:

a) l'inidoneità dell'informativa resa agli utenti, in quanto priva dell'indicazione della contitolarità del trattamento, formulata in maniera generica e approssimativa con informazioni poco chiare e incomplete. Le finalità del trattamento non erano specificate, i riferimenti ai diritti degli interessati risultavano vaghi e lacunosi e non era chiaro se gli utenti fossero obbligati o meno a fornire i propri dati;
b) la mancanza di un valido consenso al trattamento dei dati; e
c) la mancata notifica al Garante del trattamento dei dati per finalità di geolocalizzazione.

Provvedimento del Garante della Privacy n. 101 del 24 marzo 2022

Antitrust	***Tutela della concorrenza e del mercato***

Abuse of a dominant position: CJEU's qualifying criteria

According to the CJEU, the abuse of a dominant position pursuant to Article 102 of TFEU is triggered when an undertaking exploits its own resources or assets in order to

Abuso di posizione dominante: i criteri di qualificazione della CGUE

Secondo la CGUE, l'abuso di posizione dominante ai sensi dell'articolo 102 del TFUE si verifica quando un'impresa sfrutta le proprie risorse o i propri beni al fine di utilizzare la

use its position of strength on the market to prevent or hinder competition.

In this respect, the CJEU has laid down the following criteria:

a) in order to establish whether a given conduct amounts to an abuse of dominant position, it is sufficient to prove that it is capable of affecting competition on the relevant market or consumers' welfare;
b) proof of lack of restrictive effects is not per se sufficient to exclude the abusive character of a conduct;
c) a market practice considered lawful may amount to be abusive if carried out by a dominant undertaking, it produces exclusionary effects and involves means other than those considered normally competitive on the relevant market;
d) when a dominant position is abused by one or more subsidiaries, the same existence of a group of companies is sufficient to hold the parent company equally liable for the abuse. Indeed, liability is presumed if, during the contested period, almost the whole stock capital of the subsidiaries is owned, directly or indirectly, by the parent company. The latter can be exonerated only if it proves to have no control over its subsidiaries' conduct and decisions, which were taken autonomously.

CJEU, Sec. V, decision of 12 May 2022, Case C-377/20

propria posizione di forza sul mercato per impedire o ostacolare la concorrenza.

A questo proposito, la CGUE ha stabilito i seguenti criteri:

a) per stabilire se un determinato comportamento costituisce un abuso di posizione dominante, è sufficiente dimostrare che esso è in grado di pregiudicare la concorrenza sul mercato rilevante o il benessere dei consumatori;
b) la prova dell'assenza di effetti restrittivi non è di per sé sufficiente a escludere il carattere abusivo di un comportamento;
c) una pratica di mercato considerata lecita può risultare abusiva se, attuata da un'impresa in posizione dominante, produce effetti di esclusione e comporta l'impiego di mezzi diversi da quelli considerati normalmente concorrenziali sul mercato rilevante;
d) quando una posizione dominante viene abusata da una o più società controllate, la stessa esistenza di un gruppo di società è sufficiente per ritenere la società madre ugualmente responsabile dell'abuso. Infatti, la responsabilità è presunta se, durante il periodo contestato, la quasi totalità del capitale azionario delle società controllate è posseduto, direttamente o indirettamente, dalla società madre. Quest'ultima può essere esonerata solo se dimostra di non avere alcun controllo sulla condotta e sulle decisioni delle sue

controllate, che sono state prese autonomamente.

CGUE, Sez. V, sentenza del 12 maggio 2022, causa C-377/20

Corporate criminal law	Diritto penale societario

Application of market manipulation and obstruction of Consob's supervision: clarifications from the Court of Cassation

The fifth section of the Supreme Court has recently outlined the application boundaries of the offences of obstructing the functions of supervision, set forth under Article 2638 of the Civil Code, as well as of market abuse, provided by Article 185 of CFA.

Accordingly, the former is a so-called "event crime", committed when an obstruction of supervisory functions takes place and completed when an actual and significant damage occurs, which derives from an active or omissive conduct consisting in the failure to provide information to the competent supervisory authorities.

Conversely, the latter, which protects the integrity of the financial market and the investor, is deemed as a "crime of conduct" and "actual danger", consummated when the

I reati di manipolazione del mercato e di ostacolo alla vigilanza della Consob: le precisazioni della Cassazione

La quinta sezione della Corte di Cassazione ha delineato i confini applicativi dei reati di ostacolo alle funzioni di vigilanza, di cui all'art. 2638 c.c., e di manipolazione del mercato, disciplinato dall'art. 185 del TUF.

Pertanto, il primo è un c.d. "reato di evento", che si consuma nel momento in cui si realizza un ostacolo alle funzioni di vigilanza e si perfeziona con il verificarsi di un danno effettivo e rilevante, derivante da una condotta attiva o omissiva consistente nell'omissione di informazioni alle autorità di vigilanza competenti.

Viceversa, il secondo, che tutela l'integrità del mercato finanziario e dell'investitore, è considerato un "reato di condotta" e di "pericolo concreto", consumato quando la condotta è idonea a produrre un'alterazione del prezzo degli strumenti finanziari.

conduct is capable of producing an alteration in the price of financial instruments.

Supreme Court, criminal section V, decision of 4 May 2022, no. 17789

Second additional protocol to the Budapest Convention on cybercrime

In Strasbourg, on 12 May, Minister of Justice Marta Cartabia signed the second additional protocol to the Budapest Convention on cybercrime.

Budapest Convention is the main multilateral pact aimed at facilitating the fight against cybercrime and establishing an international cooperation regime; currently 66 countries, including 26 EU Member States, are parties to it.

The second protocol is the result of the need felt by all participating states to strengthen cross-border cooperation and the collection of evidence in electronic form for the purpose of criminal investigations or proceedings.

The new legal instrument aims to simplify access, by judicial authorities and the police, to electronic evidence held by internet providers. However, there remains a need to respect fundamental rights, including procedural rights in criminal matters, the right to privacy and the right to protection of personal data.

Second additional protocol to the Convention on cybercrime on enhanced co-operation and disclosure of

Cassazione penale, Sez. V, sentenza del 4 maggio 2022, n. 17789

Secondo protocollo addizionale alla Convenzione di Budapest sulla criminalità informatica

A Strasburgo, il 12 maggio scorso, il Ministro della Giustizia Marta Cartabia ha firmato il secondo protocollo addizionale alla Convenzione di Budapest sulla criminalità informatica.

La Convenzione di Budapest è il principale patto multilaterale volta ad agevolare la lotta contro la criminalità informatica e ad istituire un regime di cooperazione internazionale; attualmente ne fanno parte 66 paesi, tra cui 26 Stati membri dell'UE.

Il secondo protocollo è frutto dell'esigenza avvertita da tutti gli Stati aderenti di rafforzare la cooperazione transfrontaliera e la raccolta di prove in formato elettronico ai fini di indagini o procedimenti penali.

Il nuovo strumento giuridico propone di semplificare l'accesso, da parte di autorità giudiziarie e polizia, alle prove elettroniche detenute dagli *internet provider*. Tuttavia, permane l'esigenza di rispettare i diritti fondamentali, compresi i diritti processuali in materia penale, il diritto alla riservatezza e il diritto alla protezione dei dati personali.

electronic evidence, Council of EU, Brussels, 29 March 2022

Secondo protocollo addizionale alla Convenzione sulla criminalità informatica riguardante la cooperazione rafforzata e la divulgazione di prove elettroniche, Consiglio dell'Unione europea, Bruxelles, 29 marzo 2022

List of abbreviations

BoI: Bank of Italy
CFA: Consolidated Financial Act, Legislative Decree no. 58 of 24 February 1998, Consolidated Law on Financial Intermediation
CONSOB: The national financial markets authority
Decree 231: Legislative Decree no. 231/01
DPA: Data Protection Authority
EBA: European Banking Authority
ECB: European central bank
ESMA: European and Securities Market Authority
EU: European Union
EUCJ: European Court of Justice
GDPR: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46
Law Decree no. 82/2021: Law Decree no. 82 of 14 June 2021 Urgent provisions on cybersecurity, definition of the national cybersecurity architecture and establishment of the National Cybersecurity Agency
Legislative Decree 81/2008: Legislative Decree no. 81 of 9 April 2008 implementing article 1 of Law no. 123 of 3 August 2007 on the protection of health and safety in the workplace
Legislative Decree 11/2010: Legislative Decree No 11 of 27 January 2010, implementation of Directive 2007/64/EC on payment services in the internal market, amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC, 2006/48/EC, and repealing Directive 97/5/EC
MED: Ministry of Economic Development
MEF: Ministry of Economic and Finance
MIFID II: Directive no. 2014/65/EU on markets in financial instruments

Legenda

ABE: Autorità Bancaria Europea
BCE: Banca centrale europea
BdI: Banca d'Italia
CGUE: Corte di Giustizia Europea
CONSOB: Commissione Nazionale delle Società e della Borsa
Decreto 231: Decreto Legislativo n. 231/01
ESMA: Autorità europea degli strumenti finanziari e dei mercati
Garante Privacy: Garante per la protezione dei dati personali
GDPR: Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46
D.L. 82/2021: Decreto Legge 14 giugno 2021, n. 82 Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale
D.Lgs. 81/2008: Decreto Legislativo 9 aprile 2008, n. 81 attuazione dell'articolo 1 della legge 3 agosto 2007, n. 123, in materia di tutela della salute e della sicurezza nei luoghi di lavoro
D.Lgs. 11/2010: Decreto Legislativo 27 gennaio 2010, n. 11, attuazione della direttiva 2007/64/CE, relativa ai servizi di pagamento nel mercato interno, recante modifica delle direttive 97/7/CE, 2002/65/CE, 2005/60/CE, 2006/48/CE, e che abroga la direttiva 97/5/CE
MEF: Ministero dell'Economia e delle Finanze
MISE: Ministero dello Sviluppo Economico
MIFID II: Direttiva UE n. 2014/65 sui mercati degli strumenti finanziari
PNRR: Decreto Legge 6 novembre 2021, n. 152, recante Disposizioni urgenti per l'attuazione del Piano nazionale di

RRF: Law Decree of 6 November 2021 no. 152, entitled Urgent provisions for the implementation of the National Resilience and Recovery Facility and for the prevention of mafia infiltration, converted with amendments into Law of 29 December 2021 no. 233, published in the Official Gazette on 31 December 2021 no. 310.	ripresa e resilienza e per la prevenzione delle infiltrazioni mafiose, convertito con modificazioni nella Legge 29 dicembre 2021, n. 233, pubblicata in Gazzetta Ufficiale n. 310 del 31 dicembre 2021.
TFEU: Treaty on the functioning of the European Union	**TFUE**: Trattato sul funzionamento dell'Unione Europea
	TUF: Testo Unico della Finanza, Decreto Legislativo 24 febbraio 1998, n. 58, Testo unico delle disposizioni in materia di intermediazione finanziaria
	UE: Unione Europea

Carotenuto Studio Legale is an independent boutique law firm established in 2015 and headquartered in Rome. The Firm provides contentious and non-contentious assistance, mainly in the areas of banking and financial services regulation, corporate/M&A related matters, and finance litigation, to global financial institutions, investment firms, asset management companies and other corporations doing business in Italy.

Carotenuto Studio Legale è uno Studio legale boutique indipendente, fondato nel 2015 e con sede a Roma. Fornisce assistenza e rappresentanza in giudizio, principalmente nelle aree della regolamentazione dei servizi bancari e finanziari, diritto societario/M&A e contenzioso finanziario, ad istituzioni finanziarie globali, società di investimento, società di gestione ed altre società che operano in Italia.