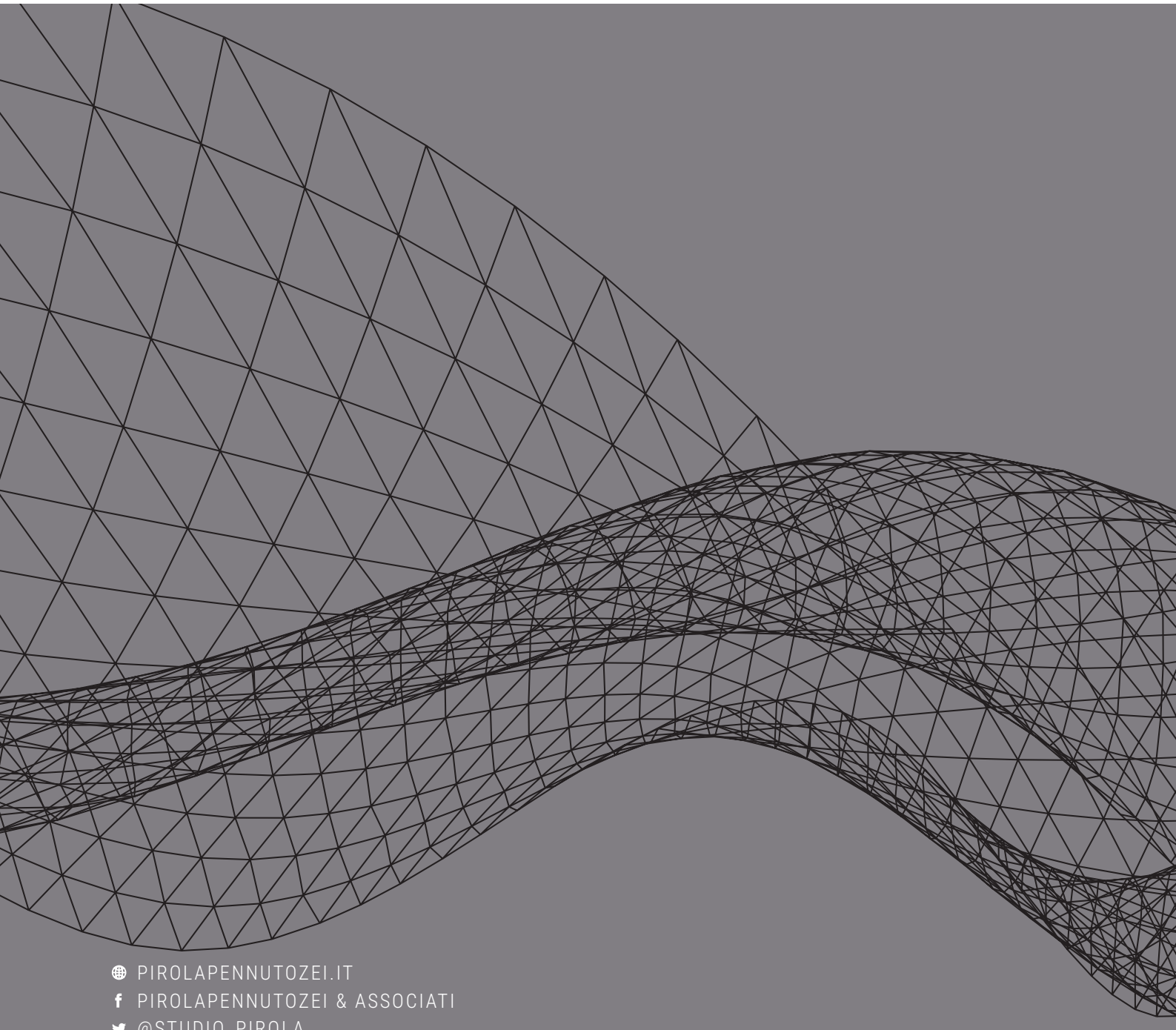
Pirola
Pennuto
Zei
& Associati

studio di consulenza
tributaria e legale

COMPLIANCE

NEWSLETTER / SETTEMBRE 2020



PIROLAPENNUTOZEI.IT
PIROLAPENNUTOZEI & ASSOCIATI
@STUDIO_PIROLA
PIROLA PENNUTO ZEI & ASSOCIATI

Pirola Pennuto Zei & Associati
studio di consulenza tributaria e legale

INDICE

NORMATIVA

PRASSI

TORNA ALL'INDICE ↑

Pirola Pennuto Zei & Associati
studio di consulenza tributaria e legale

INDICE

GIURISPRUDENZA

NORMATIVA

1.1
D.Lgs. n. 116/2020: modifiche al Codice dell'Ambiente

Lo scorso 11 settembre è stato pubblicato in Gazzetta Ufficiale il D.Lgs. n. 116/2020 recante l'"*Attuazione della direttiva (UE) 2018/851 che modifica la direttiva 2008/98/CE relativa ai rifiuti e attuazione della direttiva (UE) 2018/852 che modifica la direttiva 1994/62/CE sugli imballaggi e i rifiuti di imballaggio*".
Il provvedimento, in vigore dal 26 settembre, apporta numerose modifiche al Codice dell'Ambiente (D.Lgs. n. 152/2006). Tra i punti di interesse ai fini del D.Lgs. n. 231/2001 vi sono le modifiche in relazione alla tenuta, trasmissione e registrazione dei formulari. In particolare, il Decreto in parola ha modificato il testo dell'art. 258, comma 4, del D.Lgs. n. 152/2006, costituente reato ambientale presupposto della responsabilità amministrativa da reato degli enti.

1.2
Provvedimenti attuativi del perimetro di sicurezza nazionale cibernetica

Il Consiglio dei Ministri ha recentemente approvato, in esame preliminare, un regolamento, da adottarsi mediante decreto del Presidente della Repubblica, in attuazione delle "*Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica*" (D.L. 21 settembre 2019, n. 105).
Il regolamento, inter alia, definisce le procedure, le modalità e i termini con cui il Centro di valutazione e certificazione nazionale (CVCN) e gli altri centri individuati dalla normativa valutano i beni, i sistemi e i servizi di Information and Communication Technologies (ICT) che i soggetti inclusi nel perimetro intendono acquisire, nel caso in cui questi ultimi siano di rilevanza strategica per la fornitura di servizi essenziali e per assicurare le funzioni essenziali dello Stato.
Recentemente, inoltre, le Commissioni competenti di Camera e Senato hanno espresso parere favorevole con osservazioni sullo Schema di decreto del Presidente del Consiglio dei ministri in materia di perimetro di sicurezza nazionale cibernetica.
Lo schema, in particolare, dà attuazione a due previsioni delle "*Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica*", aventi ad oggetto: *(i)* le modalità e i criteri procedurali di individuazione di amministrazioni pubbliche, enti e operatori pubblici e privati inclusi nel perimetro di sicurezza nazionale cibernetica che, per questo, saranno tenuti al rispetto delle misure e degli obblighi previsti dal decreto legge; *(ii)* la definizione dei criteri con i quali i soggetti, inseriti nel perimetro di sicurezza nazionale

cibernetica, predispongono e aggiornano l'elenco delle reti, dei sistemi informativi e dei servizi informatici di rispettiva pertinenza, comprensivo della relativa architettura e componentistica, rilevanti per le finalità della normativa introdotta dal decreto-legge e in relazione ai quali opereranno le misure e gli obblighi da essa previsti.

1.3
Iniziata la discussione sul Disegno di legge recante attuazione della Direttiva UE sulla lotta al riciclaggio mediante il diritto penale

A inizio ottobre ha avuto avvio la discussione generale sul Disegno di Legge n. 1721, recante la "*Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea - Legge di delegazione europea 2019*".
Tra i provvedimenti comunitari che dovranno essere attuati vi è la Direttiva UE 2018/1673 del 23 ottobre 2018 sulla lotta al riciclaggio mediante il diritto penale, finalizzata a rendere la cooperazione transfrontaliera fra le autorità competenti più efficiente e più rapida. La Direttiva tratta anche la disciplina della responsabilità amministrativa da reato degli enti, richiedendo l'adozione da parte degli Stati membri, di misure volte ad estendere agli enti la responsabilità per il reato di riciclaggio.
Si segnala che i reati di riciclaggio e autoriciclaggio costituiscono da tempo reato-presupposto ai sensi del D. Lgs. n. 231/2001.

PRASSI

2.1

Reati tributari: le indicazioni della Guardia di Finanza

Lo scorso 1 settembre la Guardia di Finanza ha diffuso la circolare n. 216816/2020, avente ad oggetto le modifiche alla disciplina dei reati tributari e della responsabilità amministrativa degli enti.
L'ente ha, in particolare, fornito ai propri Reparti indicazioni operative sugli illeciti tributari maggiormente lesivi degli interessi erariali, considerate le recenti novità normative in materia, da ultimo il D. Lgs. n. 75/2020, che ha ampliato il catalogo delle fattispecie tributarie costituenti reato presupposto ai sensi del D. Lgs. n. 231/2001.
Il documento, dopo aver illustrato i principali novità normative, approfondisce alcune tematiche di interesse per l'esecuzione di indagini di polizia giudiziaria, tra cui la confisca allargata e l'introduzione e l'ampliamento dei reati tributari nel D. Lgs. n. 231/2001.
Da ultimo, la circolare delinea altresì le differenze tra i Modelli di organizzazione, gestione e controllo e il *Tax Control Framework,* ribadendo la non perfetta sovrapponibilità dei due istituti.

2.2

EDPB: emanate le Linee Guida sui concetti di titolare e responsabile del trattamento ai sensi del GDPR

Lo scorso 2 settembre il Comitato Europeo per la Protezione dei Dati (dall'inglese "*European Data Protection Board*" o "*EDPB*") ha sottoposto a consultazione pubblica la prima versione delle "*Guidelines 07/2020 on the concepts of controller and processor in the GDPR*", volte a fornire chiarimenti circa le caratteristiche di due figure centrali nell'ambito del GDPR: il titolare e il responsabile del trattamento.
Le Linee Guida, che riprendono le "*EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725*", chiariscono, ad esempio, che il rapporto contrattuale può risultare utili al fine di individuare il titolare del trattamento anche in assenza di accesso ai dati personali.
L'EDPB si è altresì soffermato sulla controversa figura dei contitolari del trattamento, precisando che, ai fini della sussistenza della contitolarità, è necessario che sia impossibile effettuare il trattamento senza la partecipazione di entrambe le parti, che devono determinare congiuntamente le finalità e i mezzi del trattamento.
Il periodo di consultazione pubblica terminerà il prossimo 19 ottobre.

2.3

Le Linee Guida EDPB sul *targeting* nel contesto dei *social media*

Lo scorso 2 settembre, l'EDPB ha sottoposto a consultazione pubblica le "*Guidelines 8/2020 on the targeting of social media users*", finalizzate a fornire una regolamentazione completa delle attività di targeting degli utenti dei *social media* – ovverosia l'indirizzamento di specifici messaggi agli utenti dei social media al fine di promuovere i propri interessi commerciali, politici o di altro tipo –, che spesso si sono rivelate problematiche ai fini della normativa in materia di protezione dei dati personali.
Le Linee Guida nello specifico: *(i)* individuano i diversi meccanismi di *targeting* diffusi nella prassi commerciale e le relative basi giuridiche; *(ii)* identificano i ruoli e le responsabilità dei soggetti coinvolti nelle attività di targeting (i.e. utenti, *social media provider, targeter* e altri attori rilevanti quali, ad es., agenzie di *marketing*), con un *focus* particolare sulla contitolarità; *(iii)* definiscono il contenuto degli accordi di contitolarità; *(iv)* illustrano le misure da porre in essere al fine di garantire la protezione dei dati personali; e (v) analizzano i rischi per gli interessati.
Il periodo di consultazione pubblica terminerà il prossimo 19 ottobre.

2.4

Garante Privacy: sanzione da 80.000 Euro ad una nota azienda ospedaliera campana

Con il "*Provvedimento del 17 settembre 2020 [doc. web n. 9461168]*", l'Autorità Garante per la protezione dei dati personali ha comminato una multa da 80.000 € ad una nota azienda ospedaliera campana in quanto aveva trattato illecitamente i dati personali di oltre 2.000 aspiranti infermieri, i cui dati (inclusi quelli relativi alla salute) erano liberamente accessibili tramite il portale web dedicato alla gestione delle candidature.
Ad esito delle indagini, il Garante ha accertato che, a causa dell'errata configurazione dei sistemi informativi dell'ospedale, collegandosi al suddetto portale venivano visualizzati "*in chiaro*" i codici assegnati ai candidati al momento dell'iscrizione al concorso, tramite i quali era possibile accedere all'area del portale nella quale erano contenuti i documenti presentati dai partecipanti, consentendo addirittura di modificare i dati personali inseriti dai concorrenti.
Il Garante ha pertanto riscontrato una violazione del GDPR in capo all'ospedale, il quale: *(i)* non aveva adottato misure tecniche e organizzative idonee a garantire la sicurezza e l'integrità dei dati personali; *(ii)* non aveva reso alcuna informativa in favore degli interessati; *(iii)* non aveva regolamentato con atto

scritto i rispettivi ruoli e responsabilità nel contesto dei rapporti con il fornitore a cui era stata affidata la gestione della piattaforma, il quale, tra l'altro, aveva continuato a trattare i dati oggetto di violazione anche dopo la cessazione del rapporto.
Pertanto, l'Authority ha comminato una sanzione da 80.000 € all'azienda ospedaliera, e una sanzione da 60.000 € al fornitore che gestiva la piattaforma.

2.5

Accesso civico e dati sanitari: il provvedimento del Garante Privacy

Con il "*Parere su istanza di accesso civico - 3 settembre 2020 [doc. web n. 9461036]*", l'Autorità Garante per la protezione dei dati personali ha chiarito che l'accesso civico ai sensi del D.Lgs. n. 33/2013 non può riguardare dati relativi alla salute che consentano di identificare gli interessati, anche indirettamente.
Il Garante, in particolare, era stato adito da un Responsabile per la Prevenzione della Corruzione e della Trasparenza di una Regione che aveva negato parzialmente l'accesso a dati relativi alla situazione epidemiologica regionale da virus COVID-19 ad un giornalista che ne aveva fatto richiesta.
In particolare, il giornalista aveva chiesto i dati suddivisi per Comune, sesso, età, esito, domicilio, data delle diagnosi di infezione, numero ed esiti dei tamponi eseguiti per paziente, distribuzione per Comune e dati relativi alle telefonate pervenute all'apposita struttura della Regione, nonché le persone prese in carico per infezione da COVID-19. A fronte di tale richiesta, la Regione, al fine di evitare che le persone contagiate venissero identificate, aveva accordato solamente un accesso parziale, fornendo alcuni dati in forma aggregata e negando l'accesso ad altri.
Ad esito dell'istruttoria, il Garante ha ritenuto corretto l'operato della Regione, ravvisando la possibilità per il giornalista di identificare gli interessati qualora fossero stati forniti tutti i dati richiesti.
Da ultimo, l'Autorità ha anche sottolineato che l'accesso civico è escluso per i dati personali relativi alla salute.

GIURISPRUDENZA

3.1

Adempimenti in materia di salute e sicurezza sul luogo di lavoro: l'obbligo formativo

Con la sentenza n. 26813/20, depositata in cancelleria lo scorso 28 settembre, la Corte di Cassazione è intervenuta sul tema dell'obbligo di assicurare una formazione adeguata in materia di salute e sicurezza ai propri dipendenti da parte del datore di lavoro.
Quest'ultimo, in particolare, veniva condannato per l'omessa adeguata formazione di una dipendente assunta con le mansioni di addetta al magazzino e carrellista.
Il ricorrente, tuttavia, impugnava la sentenza in quanto il Tribunale aveva omesso di considerare che la lavoratrice non aveva mai mantenuto una stabile mansione all'interno dell'azienda, avendo manifestato in più circostanze problemi di salute che non avevano consentito di individuare per lei una collocazione idonea.
La Corte ha rigettato il ricorso, statuendo che "*l'assegnazione di mansioni diverse alla dipendente, lungi dall'avere natura esimente, rendeva in realtà ancor più stringente l'esigenza di assicurare alla stessa un'attenta formazione sui rischi connessi all'attività svolta*".
Pertanto, la Cassazione ha determinato che il datore di lavoro aveva violato l'obbligo di aggiornamento formativo previsto dall'art. 37, comma 1, del D. Lgs. n. 81/2008.

3.2

La Corte di Cassazione si pronuncia in materia di dichiarazione fraudolenta mediante altri artifici

Lo scorso 2 luglio, la Corte di Cassazione – con la sentenza n. 26089/2020 – rigettava il ricorso proposto avverso un'ordinanza del Tribunale del Riesame di Cosenza, confermando il sequestro preventivo, finalizzato alla confisca di beni immobili, di beni mobili registrati e di disponibilità finanziarie fino alla concorrenza della somma pari al profitto dei reati di dichiarazione fraudolenta mediante altri artifici e di indebita compensazione, di recente introdotti nel catalogo dei reati presupposto della responsabilità amministrativa degli enti.
Il caso in esame vede implicato un commercialista, ritenuto responsabile in concorso con gli amministratori delle società coinvolte nella commissione dei reati contestati. In particolare, la Corte confermava che le dichiarazioni IVA inviate erano risultate false, in quanto frutto di un meccanismo fraudolento in cui erano coinvolte alcune società rivelatesi quasi tutte inesistenti.

Di conseguenza, la Cassazione respingeva il ricorso sulla base del fatto che il commercialista aveva "*fornito un apprezzabile contributo al compimento delle attività illecite, avendo lo studio (ndr. di cui era titolare) provveduto all'invio telematico delle false dichiarazioni IVA, apponendovi un visto di conformità di sicuro mendace, in quanto il professionista incaricato aveva omesso qualsivoglia controllo, non trattenendo peraltro copia della documentazione contabile*".

3.3
La Cassazione delinea il confine tra trasparenza nella P.A. e privacy

Con la sentenza n. 18292/2020, depositata in cancelleria lo scorso 3 settembre, la Corte di Cassazione ha chiarito il discrimine tra la disciplina della *privacy* e quella della trasparenza nella P.A. ex D.Lgs. n. 33/2013.
Nel caso di specie, un Comune aveva adito la Suprema Corte al fine di vedersi disapplicata una sanzione comminatagli dall'Autorità Garante per la protezione dei dati personali a causa della pubblicazione dei dati personali di una dipendente comunale coinvolta in un contenzioso per oltre 15 giorni, periodo necessario di pubblicazione delle delibere comunali nell'albo pretorio.
La Corte, rigettando il ricorso promosso dal Comune, ha puntualizzato che la violazione non riguardava di per sé la pubblicazione dei dati personali della dipendente comunale, pienamente legittima, ma, bensì, l'omessa rimozione degli stessi una volta trascorsi i 15 giorni previsti dalla normativa.
La sentenza in esame, infine, effettua anche un interessante parallelismo con la disciplina del D.Lgs. 231/2001, ravvisando in capo al Comune una colpa di organizzazione simile a quella di cui alla disciplina in materia di responsabilità amministrativa degli enti.

3.4
Accesso abusivo a sistemi informatici e violazione dei limiti dell'autorizzazione

La Corte di Cassazione, nella sentenza n. 25944 depositata lo scorso 11 settembre, ha ribadito l'orientamento assunto dalle Sezioni Unite sulla irrilevanza, ai fini dell'integrazione del reato, delle finalità perseguite nella condotta di accesso abusivo ad un sistema informatico o telematico di cui all'art. 615-ter c.p., costituente reato presupposto della responsabilità amministrativa degli enti.
La sentenza, in particolare, confermava la condanna di un agente di polizia che si era introdotto nel sistema SDI in uso alle forze dell'ordine – al cui accesso era abilitato – al fine di reperire informazioni concernenti una controparte contrattuale del cognato e, pertanto, per una finalità privata.

La Cassazione, con l'occasione, richiamava il principio di diritto per cui "*integra il delitto previsto dall'art. 615-ter cod. pen. la condotta di colui che, pur essendo abilitato, acceda o si mantenga in un sistema informatico o telematico protetto violando le condizioni ed i limiti risultanti dal complesso delle prescrizioni impartite dal titolare del sistema per delimitarne oggettivamente l'accesso, rimanendo invece irrilevanti, ai fini della sussistenza del reato, gli scopi e le finalità che abbiano soggettivamente motivato l'ingresso nel sistema*".

Pirola
Pennuto
Zei
& Associati
studio di consulenza
tributaria e legale

Via Vittor Pisani, 20
20124 Milano

T. +39.02.669951
F. +39.02.6691800

info@studiopirola.com
www.pirolapennutozei.it

COMPLIANCE NEWSLETTER | SETTEMBRE 2020

RIFERIMENTI NORMATIVI, PRASSI E GIURISPRUDENZA AL 30 SETTEMBRE 2020.
LA PRESENTE NEWSLETTER ILLUSTRA LE PRINCIPALI NOVITÀ E ALCUNE QUESTIONI DI INTERESSE GENERALE, E RAPPRESENTA DUNQUE UNO STRUMENTO MERAMENTE INFORMATIVO, IL CUI CONTENUTO NON VA UTILIZZATO COME BASE PER EVENTUALI DECISIONI OPERATIVE.
PER ULTERIORI INFORMAZIONI, VI INVITIAMO A CONTATTARE IL VOSTRO PARTNER DI RIFERIMENTO O AD INVIARE UN'EMAIL A UFFICIOSTUDI@STUDIOPIROLA.COM