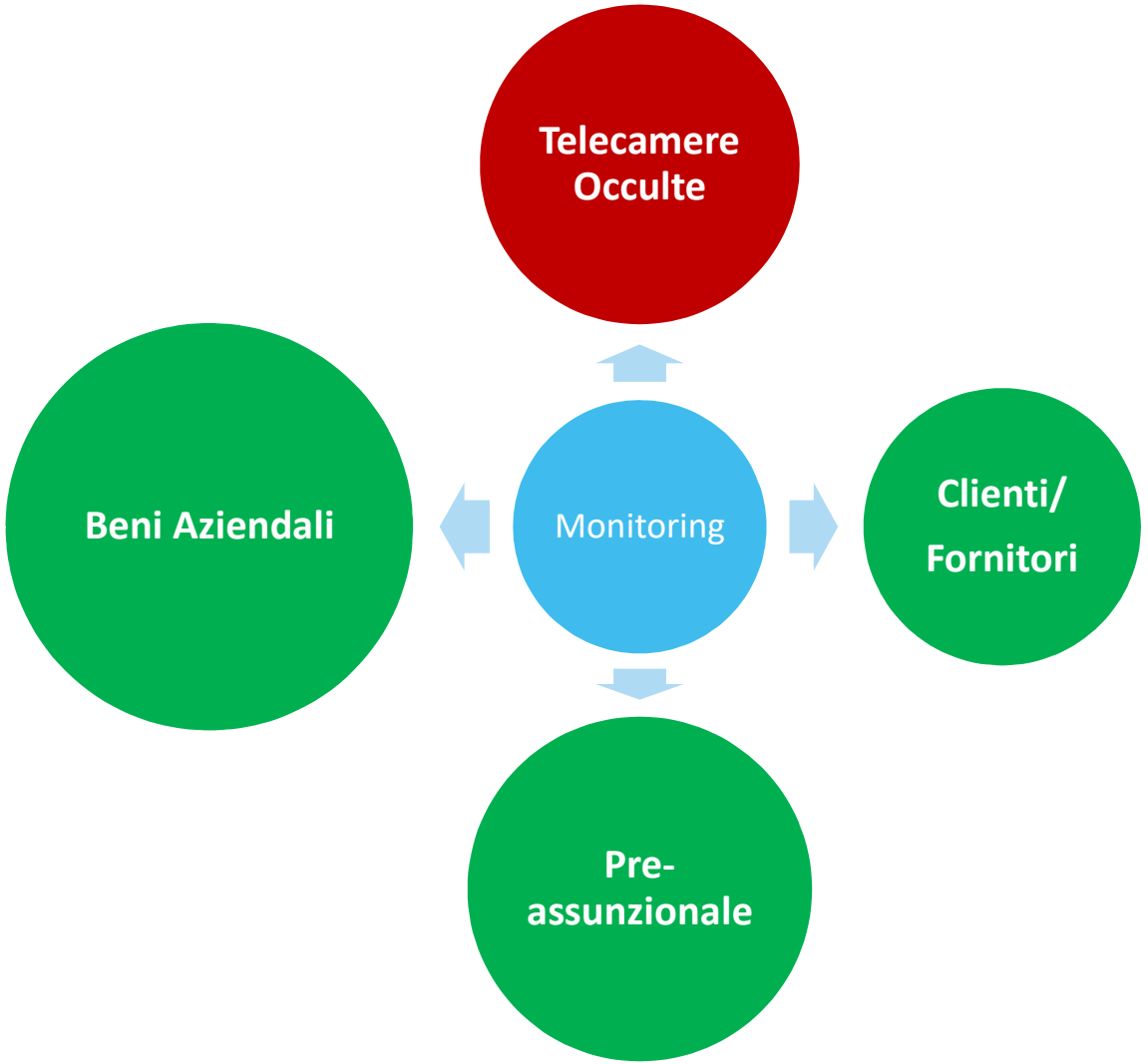
DEFENSIS

MILANO, 12 SETTEMBRE 2019

TECNOLOGIA, LAVORO E CONTENZIOSO

DEFENSIS


Telecamere Occulte
Beni Aziendali
Monitoring
Clienti/ Fornitori
Pre-assunzionale

DEFENSIS

Uso di sistemi di videoregistrazione, anche occulti

Legittimo il licenziamento per giusta causa di un dipendente ripreso a rubare da telecamere occulte

Sentenza Corte di Cassazione 10636 del 2 maggio 2017

Si è pervenuti alla affermazione di una tendenziale ammissibilità dei controlli difensivi "occulti", anche ad opera di personale estraneo all'organizzazione aziendale, in quanto diretti all'accertamento di comportamenti illeciti diversi dal mero inadempimento della prestazione lavorativa, sotto il profilo quantitativo e qualitativo, ferma comunque restando la necessaria esplicazione delle attività di accertamento mediante modalità non eccessivamente invasive e rispettose delle garanzie di libertà e dignità dei dipendenti.

Legittimi i controlli, anche a mezzo di telecamere occulte, diretti ad accertare comportamenti illeciti e lesivi del patrimonio e immagine aziendale

Sentenza Corte di Cassazione 3122 del 17 febbraio 2015

Si conferma che le garanzie poste in materia di divieto di controlli a distanza "trovano applicazione ai controlli difensivi diretti ad accertare comportamenti illeciti dei lavoratori, quando, però, tali comportamenti riguardino l'esatto adempimento delle obbligazioni discendenti dal rapporto di lavoro, e non, invece, quando riguardino la tutela di beni estranei al rapporto stesso, con la conseguenza che devono ritersi legittimi i controlli, anche a mezzo di telecamere occulte - diretti ad accertare comportamenti illeciti e lesivi del patrimonio e immagine aziendale".

https://www.defensis.it/risorse-eventi/rassegna_giurisprudenziale.html

HBR.ORG Harvard Business Review

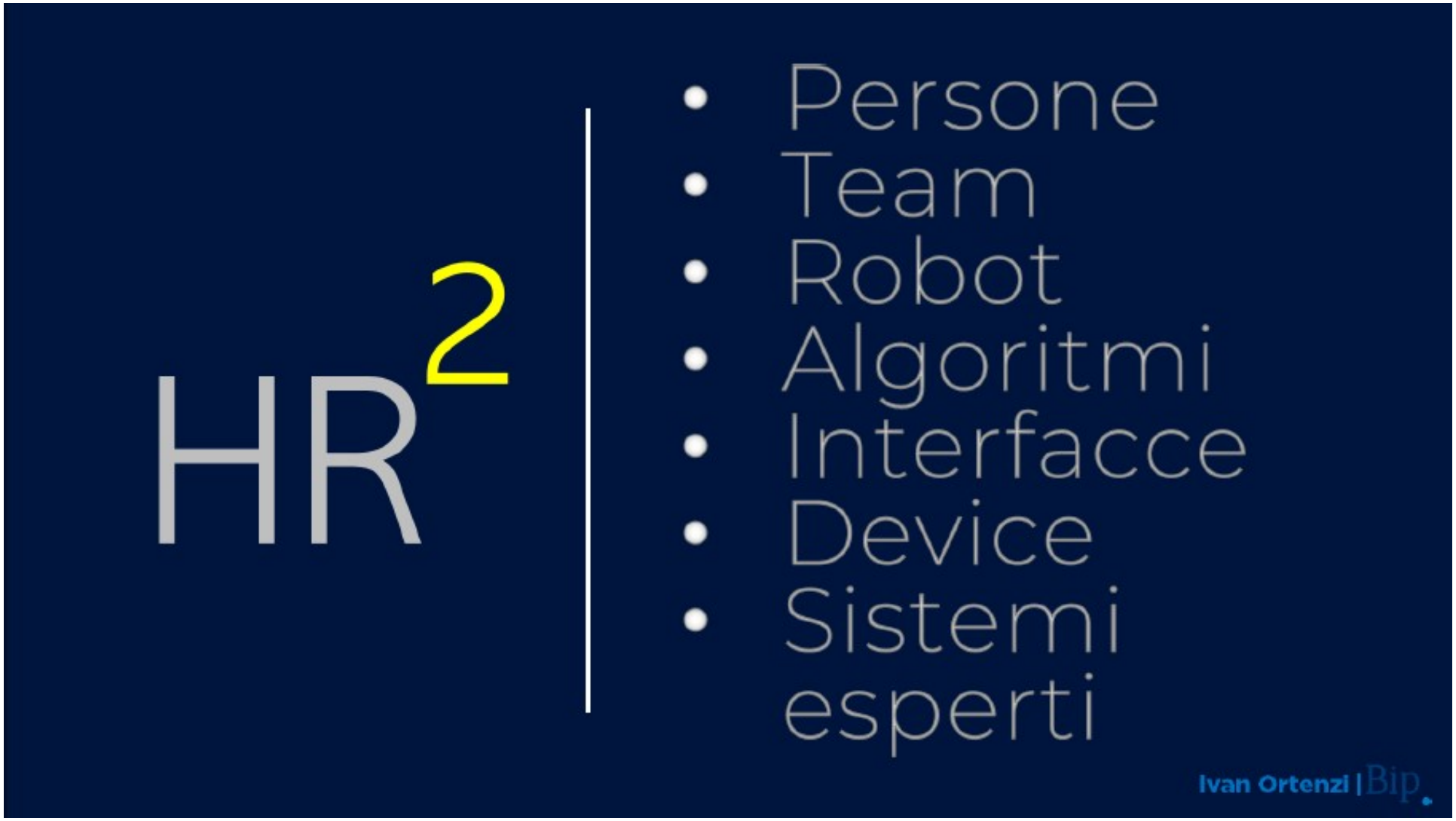
Stopping White-Collar Crime at Your Company

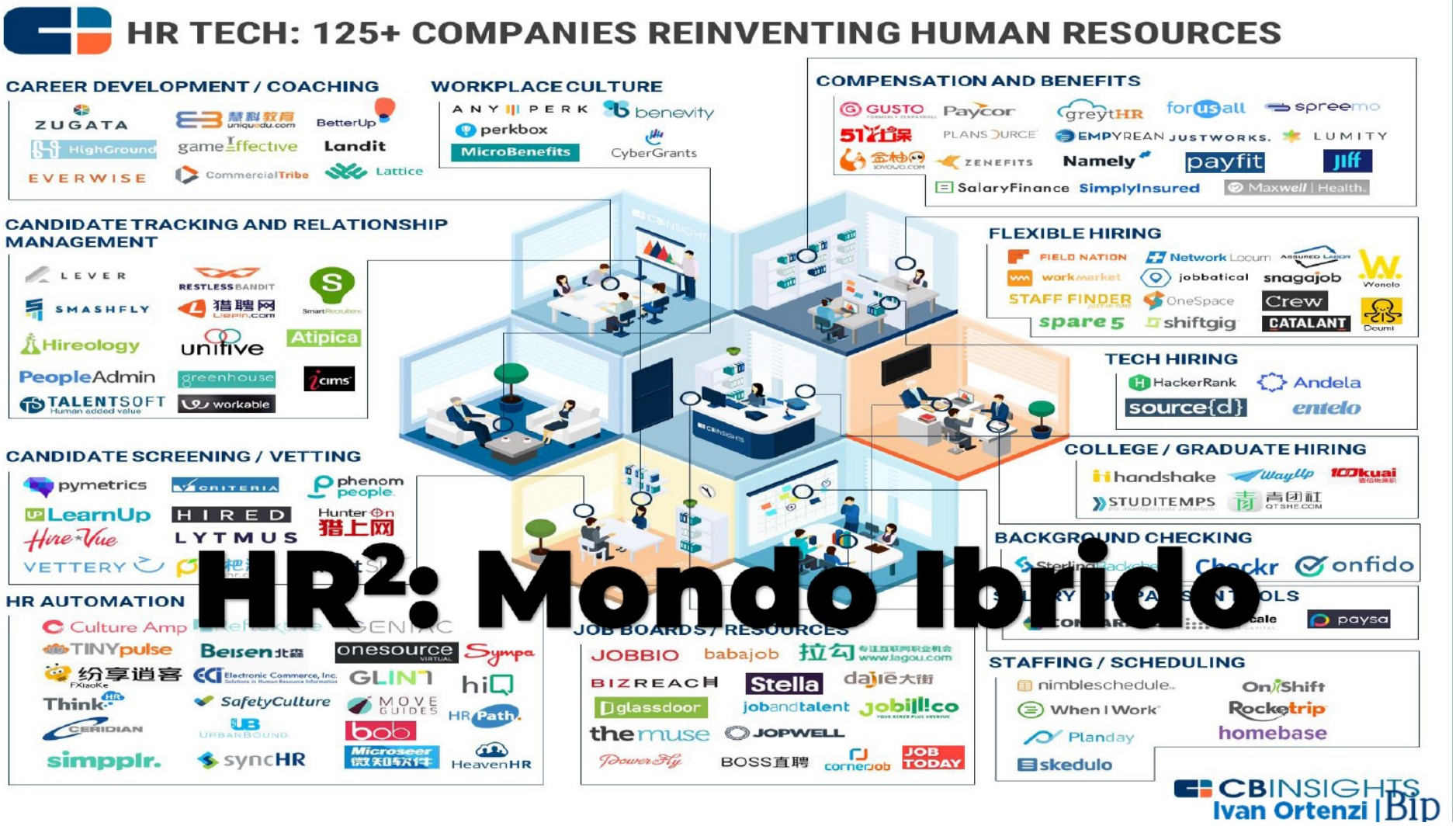
JULY 02, 2019

- Even in a single company you can have different interpretations of **ethics**
- **Geography**: working in different jurisdictions increases risks. Gdpr: rep. conseq in the US and huge fines in Europe
- You try to reach a single standard, but people come from **different cultures**
- **Three questions**: have you seen anything questionable? did you report it? if not why?
- Doing additional **Reputational Due Diligence** in certain high risk areas

https://hbr.org/ideacast/2019/07/stopping-white-collar-crime-at-your-company

«faccio molti più danni io con un mio portatile in pigiama seduto di fronte alla prima tazza di Earl Grey di quanti ne faccia tu in un anno sul campo»


HR2
Persone
Team
Robot
Algoritmi
Interfacce
Device
Sistemi esperti
Ivan Ortenzi | Bip



HR²: Mondo Ibrido

DEFENSIS

- Il collaboratore è immerso nella tecnologia già prima di entrare in azienda
- La normativa **abbandona le prescrizioni** minime (GDPR ART. 33, NIS, AGID…)
- E’ l’azienda che **sceglie misure adeguate** per proteggere il patrimonio aziendale
- Obbliga alla **notifica rapida (art 33 GDPR)** / whistleblowing
- Lo scenario tecnologico renderà **sempre più difficile agire ex post**

DEFENSIS

Aveva dei beni aziendali in uso?

DEFENSIS

Giuslavoro

ALTRA ATTIVITA' IN ORARIO D'UFFICIO

E' **previsto** che venga raccolto quel tipo di dato?

DEFENSIS

IP

FURTO DI INFORMAZIONI

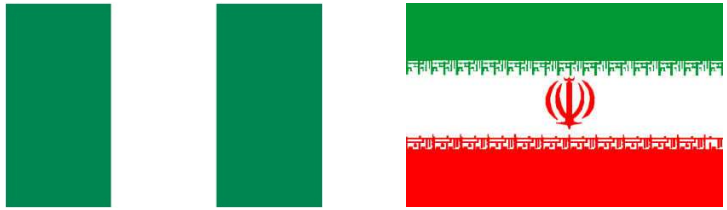
Le informazioni digitali **cancellate** possono essere irrecuperabili

Il dispositivo su cui è transitato il dato **non c'è più**

DEFENSIS

Frode e MIM

FURTO IDENTITA' e HACKING



E' **previsto** che venga raccolto quel tipo di dato?

Qualcuno verifica la sicurezza di server/applicazioni in «**cloud**»?

DEFENSIS

Il tribunale di Bari, con sentenza 2636 del 10 giugno 2019, ha deciso di ammettere come prove gli screenshot delle conversazioni Facebook, la quale rivelava alla concorrenza segreti aziendali.

La segretaria aveva installato sul cellulare aziendale l'applicazione Facebook associata ad un profilo personale. La lavoratrice, in congedo per malattia, aveva restituito il cellulare sul quale continuavano a pervenire messaggi che il datore di lavoro ha raccolto, rilevando oltre alle numerose conversazioni private anche conversazioni con la concorrenza nelle quale la segretaria rivelava informazioni aziendali riservate.

Per il giudice di Bari, le circostanze esposte sono risultate sufficienti per ammettere la giusta causa di licenziamento, **ricordando nella sentenza che il datore di lavoro può controllare i propri dipendenti per evitare possibili condotte gravose per l'azienda**.

Se **durante i controlli dei computer per motivi di sicurezza**, vengono rilevati accessi alla posta elettronica personale e a siti non attinenti alle attività lavorative, il datore di lavoro possa avviare una **contestazione disciplinare** e nullo è il ricorso al Garante della Privacy da parte del lavoratore

Corte di appello di Roma n. 1331 del 22 marzo 2019

La Gran Camera della Corte europea dei diritti dell'uomo è intervenuta in materia e – con sentenza C. 61496/08 del 5 settembre 2017 - ha stabilito che le comunicazioni personali possono essere **soggette a limitazioni solo se il dipendente sia stato preventivamente informato della possibilità, modalità e ragioni di un controllo sulla corrispondenza aziendale**.

DEFENSIS

Sentenza della Corte di Cassazione 13266/2018.

L’indagine informatica sull’utilizzo del PC (strumento di lavoro), da cui si era riscontrato un **utilizzo per finalità extra lavorative**, non si pone in violazione della normativa sui controlli a distanza di cui all’articolo 4 dello Statuto dei lavoratori (legge n. 300/70).

In questo caso la mancanza di direttive aziendali (policy) non rileva poiché l'addebito disciplinare contestato al lavoratore attiene alla violazione dei suoi doveri fondamentali di diligenza nello svolgimento dei propri compiti.Il datore abbia posto in essere verifiche dirette ad accertare comportamenti del prestatore illeciti e lesivi del patrimonio e dell'immagine aziendale: e tanto più se si tratti di controlli posti in essere ex post, ovvero dopo l'attuazione del comportamento addebitato al dipendente, quando siano emersi elementi di fatto tali da raccomandare l'avvio di un'indagine retrospettiva (Cass. 23 febbraio 2012, n. 2722), così da prescindere dalla pura e semplice sorveglianza sull'esecuzione della prestazione lavorativa degli addetti, invece diretta ad accertare la perpetrazione cl), eventuali comportamenti illeciti (poi effettivamente riscontrati) dagli stessi posti in essere (Cass. 27 maggio 2015, n. 10955);

DEFENSIS

Momento del rapporto di lavoro

1) Indagini pre-assunzionali

2) Monitoring antifrode

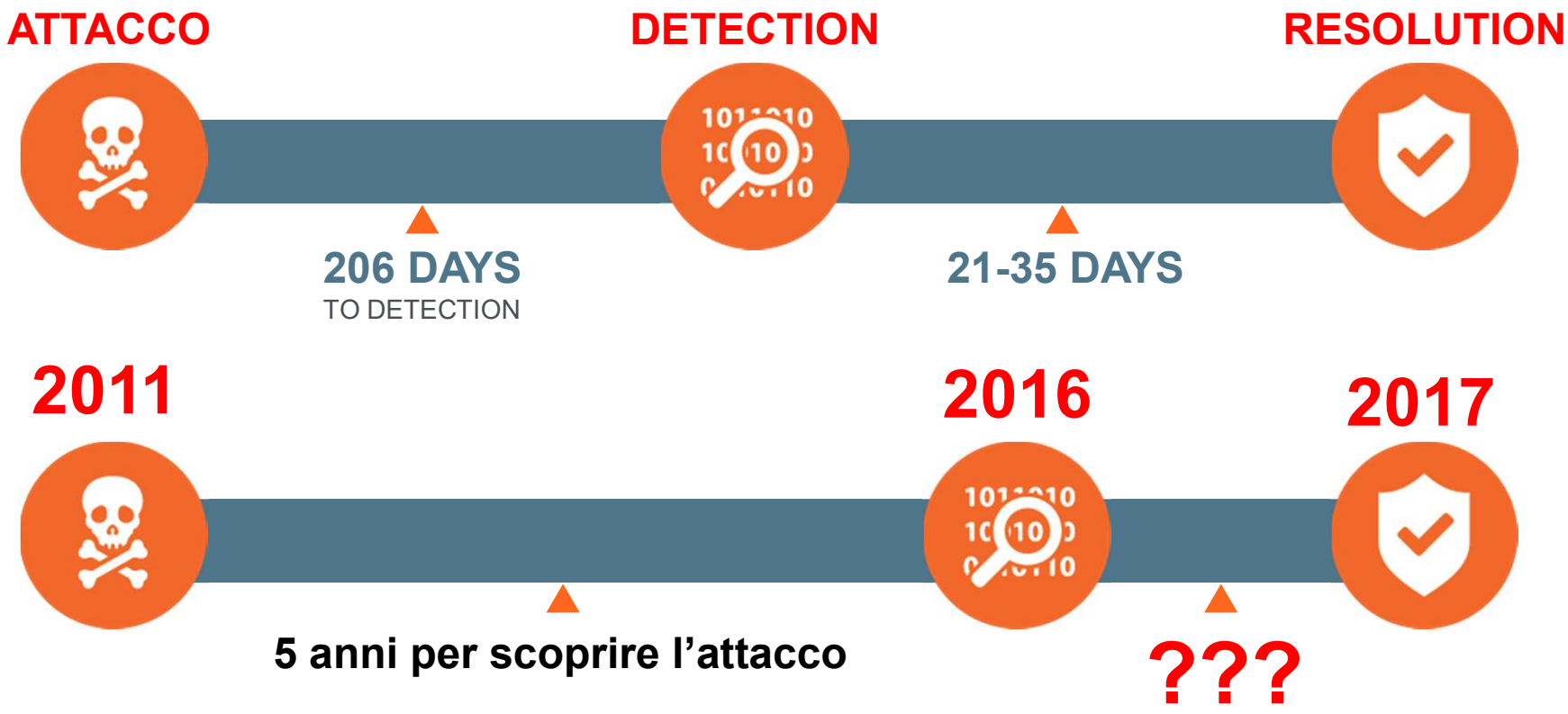
3) Investigazioni

4) Perizie Informatiche

DEFENSIS

14.3 Nella gestione dei sistemi informatici aziendali, e degli strumenti di lavoro, il servizio ICT, o **terzi** incaricati dalla direzione, potranno acquisire informazioni generate dalle funzionalità insite negli stessi sistemi, quali: i log generati da Microsoft Windows/Android/iOS, gli accessi alla rete e ai dispositivi aziendali, la cancellazione, creazione o esportazione/trasferimento di file e informazioni, l'uso di file/software di carattere non lavorativo. I dati verranno conservati per **206 giorni** e quindi cancellati. Tali informazioni potranno essere utilizzate in caso di attacco informatico, incidente informatico e ai sensi del successivo punto X, **per tutti i fini connessi al rapporto di lavoro**, sempre nell'ambito delle finalità individuate nel precedente punto Y, e con espressa esclusione di qualsiasi forma di controllo sistematico e costante nei confronti degli utenti degli stessi sistemi.

DEFENSIS


ATTACCO
DETECTION
RESOLUTION
206 DAYS
TO DETECTION
21-35 DAYS
2011
2016
2017
5 anni per scoprire l'attacco
???

Email data breach detected	SHOW	ACTIONS
Rilevata possibile cancellazione massiva nel PC PC-ALICE	SHOW	ACTIONS
Suspect file (.dwg) detected in critical path (F: G: H:)	SHOW	ACTIONS

DEFENSIS

PRE-EMPLOYMENT SCREENING / VERIFICA PREASSUNTIVA

TERMS & CONDITIONS RELATING TO THE PRE-EMPLOYMENT SCREENING PROCESS (ENG)

By signing this document, I explicitly authorize _____ (hereafter "the Company") to carry out specific pre--employment screening as indicated in this document. The pre--employment screenings are to verify (depending upon the role which I am applying for with the Company, and its seniority and sensitivity) my identity, qualifications, work experience, my ability to work with the Company in the country concerned, and that there are no important relevant factors concerning me which would lead the Company not to hire me in view of the position for which I apply.

Types of Personal Information Collected
For the purposes of pre--employment verifications, the personal information that is collected about me is provided by me on forms relating to my prospective employment with the Company. Some specific examples of this information are (i) identification and address information, (ii) education and qualifications, (iii) past employment and positions held in other organizations, (iv) professional qualifications and registrations with professional bodies, and (v) criminal convictions, and may also include (vi) financial information.

Use of My Personal Information
The Company will need to use, disclose, and transfer the

CONDIZIONI RELATIVE ALLA VERIFICA PREASSUNTIVA (ITA)

Firmando questo documento autorizzo esplicitamente _____ (qui di seguito, « la Società ») a intraprendere la verifica preassuntiva indicata nel presente documento. Le verifiche preassuntive hanno la funzione di verificare (a seconda del ruolo per il quale mi candido presso la Società, nonché alla sua posizione gerarchica e al suo grado di sensibilità) la mia identità, le mie qualifiche, la mia esperienza lavorativa, la mia capacità di lavorare presso la Società nel paese in questione, e che non vi siano fattori importanti a me relativi che potrebbero portare la Società a non assumermi in considerazione della posizione alla quale mi candido.

Tipi di informazioni personali raccolte
Ai fini delle verifiche preassuntive, le informazioni personali raccolte su di me sono quelle da me fornite sui moduli di candidatura per un'eventuale assunzione da parte della Società. Alcuni esempi specifici di tali informazioni sono (i) informazioni di identificazione e relative al mio indirizzo, (ii) istruzione e qualifiche, (iii) impieghi passati e posizioni ricoperte in altre organizzazioni, (iv) qualifiche professionali e iscrizioni a organi professionali e (v) condanne penali, e potrebbero includere anche (vi) informazioni finanziarie.

Uso dei miei dati personali
La Società avrà bisogno di usare, comunicare e trasferire le

DEFENSIS

Si sono dovuti notificare 18.478 clienti che le loro informazioni personali sono state diffuse a seguito della **violazione dell'account email** di un dipendente.

#notifica #reputazione #formazione

www.defensis.it/risorse-eventi/account_check.html

DEFENSIS

24.000 clienti coinvolti nella perdita di informazioni dovuta al **furto** di un **PC**.

#sicurezzafisica #procedure

DEFENSIS

I dati medici di 29.000 pazienti sono stati **impropriamente trattati** da parte di un dipendente del call center esterno.

#censimento #permessi

DEFENSIS

Notifica a 5.300 clienti che I loro dati sono stati disponibili online per due anni a causa di una **applicazione web non sicura**.

#vulnerability_assessment #forensic_readiness

GRAZIE

DEFENSIS

MICHELE COGO
michele.cogo@defensis.it