‘ORIENTIAMOCI’. PRIMO APPUNTAMENTO DEDICATO AL ‘LATO OSCURO DELLA PRIVACY’

«Non fidarsi, informarsi e controllare»

L’avvocato Tagliaferri e l’imprenditore Bonetti accendono un riflettore sulla gestione dei dati

di Paolo Fornasari

Privacy: come tutelarci? «L’unica maniera è non fidarsi mai, essere informati e andare a controllare. Dobbiamo sviluppare la cultura della sicurezza e mitigare il rischio del fattore umano». Questo il prezioso consiglio dell’avvocato Franco Tagliaferri, esperto in tutela della privacy, durante l’evento “Il lato oscuro della privacy” che si è svolto venerdì 20 ottobre, primo appuntamento del ciclo “Orientiamoci strumenti per la crescita delle PMI”, organizzato dal Comitato Piccola Industria dell’Associazione Industriali di Cremona, nella sede di Piazza Cadorna.

Ha introdotto l’incontro il Presidente, Paolo Aramini: «Ripensando al precedente evento, quello sul metaverso tenuto a Crema il 25 maggio, abbiamo deciso di proseguire occupandoci del digitale e oggi affronteremo il lato oscuro della privacy e la conseguente sicurezza dei dati, temi fondamentali soprattutto in questo periodo. Ci aiuterà a capire meglio la tematica e i suoi rischi, l’avvocato Tagliaferri, mentre Rodolfo Bonetti, titolare di Bonetti Costruzioni meccaniche S.r.l.”, ci illustrerà il percorso della sua azienda».

«E’ un invito che ho accolto volentieri - ha esordito l’avvocato - sia per un fattore personale, la mia profonda avversione, ormai ventennale, riguardo l’argomento, sia perché i momenti di informazione-condivisione sono la base per poterci difendere».

Tagliaferri ha sintetizzato la nascita, curiosa, della privacy: «Nel 1970 in uno Stato del Nord Europa ebbero l’idea di assegnare ad ogni cittadino un codice alfanumerico (quello che noi conosceremo nel 1974 con il codice fiscale) che nasceva dall’esigenza di curare il cittadino nel migliore dei modi possibile conoscendo le sue allergie, le malattie, le patologie… Uno scopo nobile, quindi, ma che porta ad esempio un cittadino a vedersi rifiutare un lavoro perché risulta che uno zio ha problemi psichici. Allora vengono domande e dubbi, perché quello che era uno scopo nobile contiene anche il male e qualcuno può accedere, attraverso lo strumento, ai dati». Oggi si è corsi ai ripari: «L’ultimo regolamento stabilisce che il trattamento dei dati deve esser lecito, ossia rispondere alle leggi, equo perché devo trattare solo i dati necessari per quello scopo legittimo, infine trasparente, perché l’interessato deve sapere perché si sono voluti i suoi dati e come li si usa. In sintesi: si possono prendere solo dati strettamente necessari, si deve garantire di saperli conservare in sicurezza e di cancellarli quando non servono più».

Tagliaferri ha affrontato poi il tema del consenso: «Tutte le volte che i dati vengono usati per uno scopo diverso rispetto a quello per cui sono stati rilasciati, è necessario acquisire il consenso. Per dirvi come questo si rifletta sulla vita quotidiana, il crimine sceglie di rivolgersi alle persone fisiche, perché sono le più facili da abbindolare, per poi arrivare ad avere anche i dati aziendali. Vediamo il discorso sui cookies, che ci pongono davanti a quella che sembra una nostra scelta: accettare tutto, non accettare o accedere alle preferenze. L’esperienza è che troviamo flagato (contrassegnato, nda) il banner dei cookies necessari, mentre tutti gli altri non lo sono. Prestando attenzione, ci accorgiamo anche che, se proviamo ad andare su siti di alcuni giornali nazionali, non abbiamo nemmeno quella alternativa: o li accettiamo tutti o ci abboniamo, e questo è veramente inquietante. Così, la questione più importante riguarda il doverci difendere da tutte le minacce, più o meno nascoste».

Best practise in azienda

Cambiare frequentemente le password, essere dotati di doppio telefono con antivirus e crittografare i laptop

Il giurista è passato quindi a trattare un altro aspetto preoccupante, quello relativo alle fughe di dati: «Navigando in internet, di solito si visita il cosiddetto surface web, che comprende Google, Facebook, Blogs, Ecommerce YouTube Wikipedia, Website, ma che è solo lo 0,03 dell’intero web. Tutto il resto è deep web, un posto dove ci sono pagine legittime, dove si accede con nickname e password, ma c’è anche quel piccolo spazio, il dark web, che è quello che ci deve preoccupare, perché fornisce dati agli hacker, ed è qui che dobbiamo saperci difendere. È però anche giusto dire che nel dark web c’è anche del bene, perché tutti coloro che studiano il male ci entrano per scoprire le nuove strategie per contrastare le truffe e le incursioni degli hacker. Nella recente evoluzione l’attacco è sempre più personalizzato, perché ormai la raccolta dati è sempre più specifica. Un classico esempio: se si compra un articolo online, nei giorni successivi può capitare di trovarci segnalazioni dei migliori dieci pezzi dell’articolo cercato e sicuramente c’è un banner cliccando sul quale ci si può trovare col computer bloccato e per sbloccarlo bisogna pagare».

Tagliaferri ha analizzato altri esempi, perché le truffe sono tante: «Ci sono quelle che utilizzano i QRCode e in merito vi racconto un caso davvero inquietante: ne comparvero sulle vetrine di un ristorante proposti come menu, invece servivano per rubare i dati del telefonino. Ci sono anche le telefonate con cui ci vengono chiesti direttamente alcuni dati o di accedere ad alcune app…Pronto sono la sua banca e la cosa incredibile è che compare proprio il numero della banca: accettando di accedere all’app, riescono a reperire i nostri dati. Per non parlare della frontiera degli sms che è veramente variegata: vi sarà capitato di ricevere messaggi di una società di corrieri dove si dice che la consegna non è andata a buon fine e che bisogna fare un piccolo pagamento: è chiaramente da non cliccare, perché è una truffa e pagare la somma richiesta consente loro di accedere ai dati del telefonino. Tutto questo ci dice che se non siamo particolarmente attenti, non è difficile cascare nei trabocchetti tesi. Un altro problema è quello che si verifica quando dei tecnici vengono nelle aziende per una riparazione, perché il 37,5% degli addetti all’assistenza curiosa nei dispositivi dei clienti, quindi anche in questo caso occorre particolare attenzione. Penso anche a quando si porta il telefonino nei negozi per riparare lo schermo e a volte i tecnici ci chiedono il pin: può essere per pura curiosità e non per una questione di crimine vero e proprio, però la percentuale di chi lo fa è davvero elevata e non tutti sono onesti. In caso di riparazione del computer, invece, bisogna ricordarsi di fare il backup, usare software di criptografia, cancellare dati personali, non condividere la password, cioè consegnare un computer anonimo, anche se capisco l’enorme difficoltà. Anche per il telefonino, bisogna fare un backup, altrimenti ci affidiamo esclusivamente alla fiducia nell’altro, così dobbiamo pure ricordiamoci che le colonnine che usiamo negli aeroporti, hotel e centri commerciali per ricaricare la batteria, può succedere che rubino i dati del telefonino. Un altro caso ancora: alcuni dipendenti di una nota casa automobilistica spiavano i clienti attraverso le telecamere del veicolo, conservando e scambiandosi dati e probabilmente li portavano anche fuori dal sistema. Infine, voglio segnalarvi il caso delle cosiddette truffe romantiche, così chiamate perché fatte su siti di incontri».

L’avvocato Franco Tagliaferri (a destra) con Rodolfo Bonetti durante il primo appuntamento del format lanciato dal Comitato Piccola Industria di Cremona – ‘Orientiamoci. Strumenti per la crescita delle PMI’ intitolato ‘Il lato oscuro della Privacy’

IL TRATTAMENTO

Deve esser lecito, (rispondere alle leggi), equo (deve gestire solo le informazioni necessarie) e trasparente, (l’interessato deve sapere perché si sono voluti i suoi dati e come li si usa)

L’avvocato ha terminato con alcuni consigli: «Chiudo, anche se mi rendo conto che non è possibile prepararvi ad affrontare tutti i casi, perché sempre più di frequente veniamo a conoscenza di nuove strategie. Quello che cerchiamo di fare è aiutarvi ad essere pronti a cogliere nuovi modi di violazione dei nostri dati e determinante è la consapevolezza del pericolo per cui è il fattore umano che fa la differenza. Posso avere, infatti, il sistema più sicuro ma, se clicco sulla mail o sul messaggio, la truffa, che prevede sempre la vittima come complice, è fatta. L’unica maniera è non fidarsi mai, essere informati e andare a controllare. Dobbiamo sviluppare la cultura della sicurezza e mitigare il rischio del fattore umano. Bisogna, perciò, condividere le informazioni, i comportamenti corretti e le abitudini virtuose: tutto deve esser in armonia».

Nella seconda parte dell’evento, il relatore ha posto qualche breve domanda al signor Bonetti verificando con molto piacere che la sua azienda rappresenta davvero un caso virtuoso, perché attua tutte le pratiche per evitare le fughe di dati. Il titolare della Bonetti costruzioni ha infatti spiegato: «Abbiamo deciso di sposare il paradigma Industria 4.0, ma questo ha portato tante complicazioni di tipo pratico. Abbiamo perciò cercato di applicare in azienda tutte le buone pratiche che il GDPR (l’ultimo nuovo regolamento europeo sulla privacy, nda) ha condiviso, come per esempio il cambiare frequentemente le password, l’esserci dotati tutti di doppio telefono con antivirus e crittografare i laptop. Riceviamo attacchi tutti i giorni, spesso li condivido con i dipendenti, esortandoli a prestare la massima attenzione. Abbiamo capito che l’approccio alle pratiche avviate deve essere continuativo e ogni anno stanziamo una parte del budget per la sicurezza informatica e abbiamo una persona addetta all’home banking».