LA LEGGEREZZA NELLA GESTIONE DEL DATO

di UMBERTO RAPETTO, Generale (R) della Guardia di Finanza – cyber security advisor

PER RAGIONI PROFESSIONALI O PER ESIGENZE INDIVIDUALI, LA PANDEMIA HA CONDOTTO A RIVERSARE IN RETE GRANDI VOLUMI DI INFORMAZIONI, SENZA PERÒ CONOSCERNE IL DESTINO. LE CASISTICHE DI UTILIZZO DELLA TECNOLOGIA SONO MOLTO AMPIE MA TUTTE CARATTERIZZATE DALL'URGENZA, DALL'INGENUITÀ E DALLA MANCANZA DI CONSAPEVOLEZZA DEI RISCHI PER LA PRIVACY

Qualcuno dice di aver vissuto una stagione difficile. Qualcun altro, forse meno ottimista, spera in una *primavera* che secondo molti non ha, né avrebbe potuto, coincidere con il calendario.

In uno scenario internazionale confuso e forse fin troppo legittimamente frastornato dalla pandemia e dalle sue riverberazioni sanitarie, economiche e sociali, si staglia una problematica che poco va d'accordo con l'emergenza che da mesi stiamo vivendo.

La propagazione del contagio ha sconquassato il nostro vivere quotidiano, modificando le abitudini, condizionando i comportamenti e le relazioni, interferendo nei cicli produttivi e commerciali, entrando a gamba tesa nelle procedure che quotidianamente scandiscono il lavoro, la scuola, la vita famigliare.

Il distanziamento interpersonale si è rapidamente profilato come il rimedio naturale al diffondersi del virus, l'isolamento come la barriera estrema per fermare la staffetta di contagiati e di asintomatici. Quasi non ci fosse chi praticasse da tempo (e con successo) modalità di lavoro a distanza, è iniziata la virtualizzazione dei rapporti di impiego, della didattica, del fare la spesa, del parlare con il medico o con altro esperto, e così a seguire nelle infinite situazioni di una qualsivoglia giornata di chicchessia.

LA RETE E IL SUPERAMENTO DELLE DISTANZE

Il ricorso a computer, tablet e smarphone è stato pressoché immediato: una sorta di passaggio evolutivo inevitabile, una specie (per i digiuni di progresso) di primo passo sulla Luna (a quello somigliante solo per la goffaggine dell'andatura di certi utenti sbigottiti da tanta meraviglia).

L'utilizzo anche improprio di certi strumenti e l'affidarsi ciecamente alle reti disponibili ha segnato un'alba memorabile nella storia del nostro Paese e, consoliamoci, di tante altre nazioni in ambito comunitario e non.

Pur di non perdere contatto con il resto del mondo, c'è chi ha subìto l'imposizione di utilizzare questo o quel software o di affidarsi a piattaforme sconosciute. La casistica è di ampiezza oceanica, ma il fattore comune delle più elementari preoccupazioni è stato unanimemente riconosciuto nei dati personali che ciascuno, per ragioni professionali o per esigenze individuali, ha riversato in Rete senza conoscerne il destino.

Il guado tra reale e telematico è stato affrontato con la stessa nonchalance con cui Mister Magoo – il vecchietto ipovedente dei cartoon degli anni 60 e 70 – si metteva al volante e affrontava il traffico. Nessuno si è reso conto

dei rischi cui si andava incontro: la mancanza di indirizzo ha caratterizzato in modo uniforme il mondo pubblico e quello privato, certificando un passaggio maldestro verso un presunto *futuro*.
Il vuoto culturale ai più diversi livelli e l'impreparazione tecnica e organizzativa ha fatto confondere un semplice collegarsi da casa con un ben più aulico *smart working* (quanto ci è piaciuta questa espressione…) che, purtroppo, molto di rado si è mostrato *intelligente* ed efficace.
Lo stato di necessità e le urgenze che si è portato dietro il Covid-19 hanno fatto dimenticare la delicatezza delle informazioni veicolate online e poi, incredibile dictu, hanno fatto emergere il ciclopico iceberg della *riservatezza dei dati personali*.

***Umberto Rapetto**, Generale (R) della Guardia di Finanza – cyber security advisor*

PRIVACY, SECURITY, SECRECY…

La questione della privacy (a breve distanza di tempo dall'effettiva entrata in vigore del Regolamento europeo in materia, o Gdpr che dir si voglia) ha avuto un impatto estremamente significativo su parecchi fronti e, dopo un brioso avvio di alcuni *modus vivendi* improntati su una certa leggerezza, ha determinato una serie di ripensamenti che il più delle volte non hanno condotto a utili soluzioni ma semplicemente a banali rallentamenti o a drastici stop.
Le aziende hanno spalancato le porte dei rispettivi sistemi informativi per consentire l'accesso dei propri dipendenti in grado di operare altrove (da sedi distaccate o dal salotto di casa, poco importa). Il primo elemento critico è stata la disponibilità di apparecchiature idonee: poche realtà avevano dotato il personale di computer portatili, di tablet o di smartphone prevedendone la prestazione lavorativa in mobilità.
L'agire in fretta e furia e un eccesso di semplificazione dei problemi ha nuociuto non solo alla privacy del singolo ma anche e soprattutto alla sicurezza dell'organizzazione cui lei o lui appartengono. Mentre tutti si riempiono la bocca del termine *cybersecurity* e per lavarsi la coscienza magari spendono fior di quattrini in consulenze, progetti e acquisti, il *remote working* (guai a definirlo *smart*) finisce con assumere il ruolo di trampolino per un triplo salto carpiato in una vasca che nessuno si è ricordato di riempire d'acqua.
In questo dannato periodo la necessità di "sbloccare tutto" ha avviato un processo degenerativo la cui base è la tanto osannata quanto devastante concessione del *Byod*.

E COS'È IL BYOD?

L'astrusa sigla sta per "bring your own device" e si traduce nel "prendi pure il tuo dispositivo personale".
L'autorizzazione a utilizzare lo smartphone personale non ha fatto capolino con il coronavirus, ma il rischio di contagio e la chiusura degli uffici ne hanno decretato la più ortodossa valenza. Aziende ed enti hanno conside-


© jacoblund - iStock

rato vantaggioso il non comprare attrezzature costose e destinate a rapida obsolescenza e hanno ritenuto che una simile azione garantiva l'immediata operatività della maggior parte delle risorse umane.
Datori di lavoro e dipendenti hanno così brindato al felice appianamento di qualsivoglia ostacolo a proseguire le normali attività che ciascuno garantiva per il buon funzionamento della realtà di appartenenza.
Peccato, eh già, che l'uso promiscuo di un computer o di un telefono non configuri la situazione ideale per chi vuole stare tranquillo. Un oggetto di quella specie non può essere adoperato sia per il lavoro sia per l'uso personale, perché le due sfere di utilizzo sono connotate da livelli di protezione differenti e spesso contrastanti, da esigenze di tutela non coincidenti, dalla necessità che vi sia una netta linea di demarcazione.
Uno smartphone aziendale di cui viene consentito un impiego diverso da quello *istituzionale* viene esposto a tutti i rischi che tipicamente affliggono un normale utente finale, dall'installazione di app nocive all'inoculazione di istruzioni malevole, dallo sbarco di un ransomware (uno di quei virus che determina la cifratura di tutti i file raggiungibili dal dispositivo infettato) al furto delle credenziali di accesso fino allo scippo di documenti riservati (accessibili da remoto o, peggio, scaricati per comodità sul telefonino).
Lo stesso dicasi per l'utilizzo ai fini lavorativi di un cellulare personale che potrebbe essere farcito di insidie grazie alla pregressa effervescente navigazione online o in virtù del download e dell'attivazione di applicazioni ludiche che potrebbero contenere le più bizzarre trappole.
L'utilizzazione promiscua include un ulteriore incontenibile pericolo: i figli dell'utente si prospettano come figure spettrali, incredibilmente disinibiti nel muovere i polpastrelli sul display e, nella loro spensierata immaturità, purtroppo capaci di tutto.

IL GUSTO MACABRO DELLE VIDEOCONFERENZE

Una delle pratiche che ha preso rapidamente piede è quella delle riunioni e dell'attività didattica svolte sfruttando le numerose piattaforme di incontro virtuale e di e-learning.
L'opportunità di servirsi di *Zoom* o di altra chance per


© LDProd - iStock

confrontarsi a distanza si è subito trasformata in una moda e anche piccole questioni che potevano trovare esito in due righe di mail hanno finito con l'essere l'occasione per ritrovarsi in uno dei tanti riquadri che affollavano (senza dar luogo ad assembramenti….) il monitor dei partecipanti alla call.

La gratuità di questi software e il libero accesso ai relativi canali di comunicazione ha letteralmente inebriato la collettività. Nessuno si è chiesto perché simili prodigi dovessero essere gratuiti e quindi tutti hanno cercato di approfittarne a mani basse.

Quando si è scoperto che il meeting (qualunque ne fosse la natura) era intercettabile e poteva essere indebitamente registrato da qualche malintenzionato (o semplicemente da un concorrente), qualcuno ha cominciato a riflettere sulla pericolosità della situazione. Segreti industriali e commerciali sono stati alla mercè dei banditi di turno e dei soggetti che li hanno assoldati con specifici obiettivi da perseguire.

La privacy di ciascuno, poi, è stata letteralmente calpestata e l'offerta di fruire a costo zero di servizi (dallo streaming tv all'informazione o ad altre allettanti opportunità) ha indotto a iscrizioni, registrazioni e adesioni senza che nessuno si accorgesse delle informazioni che stava rivelando e comprendesse cosa lo aspettava al termine del periodo miracoloso del *tutto gratis*.

L'INDIGESTIONE DI DATI BIOMETRICI

Il marasma tecnologico è stato amplificato da una serie di contingenze poco fortunate, figlie anch'esse dell'impreparazione ad affrontare situazioni difficili e, ahinoi, durevoli.

Le applicazioni di *contact-tracing* hanno fatto enormi scorpacciate di dati di estrema criticità (le condizioni di salute di un tizio non sono appetibili solo per il mondo dell'ospedalità privata o per le Big Pharma…), senza che ci sia stato un ritorno in termini di efficienza e di efficacia.

Le rilevazioni fatte dai termoscanner non impensieriscono per il mancato abbinamento dei soggetti sani alla temperatura, ma i febbricitanti non sempre hanno ricevuto garanzie sulla blindatura dei dati acquisiti. Qualcuno si chiede che fine fanno le delicatissime informazioni raccolte nei tanti test effettuati per scovare contagiati e asintomatici. Appena tornerà la calma sarà opportuno fare il punto della situazione, sperando che non sia troppo tardi.

POLIZZE CYBER, UN PICCOLO CONSIGLIO AL MONDO ASSICURATIVO

Questi mesi hanno messo a dura prova l'universo delle aziende e la baraonda del mandare tutti a lavorare da casa potrebbe aver compromesso le cautele dichiarate al momento della sottoscrizione di una polizza per la copertura del rischio cibernetico.

Si chiedano informazioni su cosa è successo nel periodo di lockdown: probabilmente non mancherà qualche sorpresa e forse varrà la pena tenerne conto.