GIACOPUZZI
DIRITTO D'IMPRESA

LA CULTURA DELLA SICUREZZA INFORMATICA, OLTRE IL GDPR

di Luca Giacopuzzi

(pubblicato su DIG.EAT)

GDPR: quattro lettere che ad ognuno suonano familiari, tanto si è detto del Regolamento. E ugualmente potrebbe dirsi di altri temi correlati al trattamento dei dati personali, quali per esempio il "data breach". Ma si tratta, per lo più, di una conoscenza sommaria, di superficie: prestiamo davvero attenzione alla sicurezza dei nostri dati solo dopo esserci "scottati". Eppure la sicurezza dovrebbe essere la prima preoccupazione di ogni avventura tecnologica: lo amava ripetere Einstein; ben prima, quindi, della codificazione del principio della privacy by design. E la sicurezza è un fatto culturale prima ancora che tecnologico: l'anello debole della catena della sicurezza è il fattore umano (il social engineering, del resto, sfrutta proprio questa falla). La sicurezza, se vogliamo, risiede nella capacità di comprendere il rischio, per poi capire che le misure per ridurlo - che ci sono e che spesso sono a costo zero - sono necessarie. Ma siamo fatti così: amiamo acquistare automobili dotate di sofisticati sistemi di assistenza predittiva (il volante che vibra quando si sconfina dalla carreggiata, il gas che viene tagliato quando il veicolo percepisce un pericolo) e poi vanifichiamo il tutto non allacciandoci le cinture, perché, tanto, non siamo a bordo di un aereo. Lo stesso accade in ambito informatico: riteniamo la password - il più delle volte sempre la medesima per servizi diversi - uno scudo protettivo efficace, senza eccezioni di sorta. Così non è, invece! Bisogna bandire automatismi; bisogna smettere di pensare di essere immuni ai rischi; di ritenere che il data breach (breach, con la "r", e non "data beach",

come mi è capitato di sentirmi ripetere; vabbè, eravamo a luglio: scusato!) non accada che nei film. Bisogna, soprattutto, rimettere la palla al centro. E ripartire, muovendo dai concetti di base. Per esempio dall'autenticazione. Quanti adottano l'autenticazione "a due fattori"? Pochi; e i più lo fanno, sbuffando come ciminiere, solo quando accedono ai servizi bancari. No. Serve un cambio di passo, uno scatto in avanti. Perché delegare la sicurezza del nostro ambiente informatico (sia esso il computer o un account social o altro) al solo binomio username e password ("autenticazione a un fattore") non basta davvero. E ciò non solo perché la username ha spesso la sintassi standard nome.cognome e perché la password è una combinazione spesso facilmente riconducibile all'utente, e debole (una parola di senso compiuto di 8 caratteri quando va bene; ritenendo, per giunta, di essere virtuosi perché memori dell'Allegato B al Decreto 196). Non basta, forse (ogni caso, in verità, è storia a sè), nemmeno passare dalla password alla passphrase: una frase, articolata, con maiuscole, minuscole e interpunzioni. Si proceda, invece, con l'autenticazione "a due fattori", che avviene laddove il sistema ci riconosce solo quando ad un fattore di sicurezza "che conosciamo" (la password) abbiniamo un secondo fattore, generato da un dispositivo "che abbiamo" (un SMS che riceviamo sul telefono, un OTP - OneTimePassword - che appare su un token o su una app o, ancora, un "tap" su una finestra, sempre su una app). Fino ad arrivare, ove la situazione lo richieda, ad un terzo fattore di autenticazione, biometrico: il Touch ID o il Face ID, per fare un esempio. Basta poco per avere tanto: più che uno slogan, un dato di fatto.