Alert
Innovation & New Technologies

Smart products e digital security

1. Senza bisogno di spingerci fino a sostenere che "*everything is becoming a computer*"[1] è pur vero che pochi al giorno d'oggi nel mondo industrializzato sfuggono alla definizione di utente digitale, per tale intendendosi un soggetto che faccia uso di prodotti digitali (cd *smart products*)[2].

Su questo presupposto gli utenti digitali sono classificati in "*mainstream users*" ed "*advanced users*"[3], a seconda che le loro competenze digitali siano limitate o elevate: tra i primi si annoverano in linea di massima i consumatori e le PMI, mentre tra i secondi per lo più le grandi società, oltre ai cd "*geek*" o esperti informatici. Sennonché, contrariamente a quanto si potrebbe ritenere, gli *advanced users* non sono immuni – al pari dei *mainstream users* – alle problematiche connesse alla cd *digital security*[4].

Il punto è che i prodotti digitali sono connaturatamente vulnerabili[5]: e tali vulnerabilità – che consistono in fragilità dei codici o di progettazione che possono inficiare la sicurezza del prodotto e financo dell'utente - il più delle volte sono gestite in misura meno che ottimale, quando non sono addirittura sfruttate da terzi per procurarsi illeciti vantaggi a discapito dell'utente preso di mira[6].

Si ha gestione meno che ottimale quando, ad esempio, le vulnerabilità sono il frutto del mancato adeguamento agli standard industriali ed alle *best practices* nella fase di design e progettazione del prodotto; quando il produttore ometta di inviare del tutto, o comunque tempestivamente, *security updates* relativi a vulnerabilità scoperte successivamente all'immissione sul mercato del prodotto, o quando questi vengano ignorati dal destinatario degli stessi; o, infine, in caso di utilizzo del prodotto oltre la cd *end-of-life* (EOL), e cioè oltre il ciclo di vita indicato dal produttore (quando cioè il prodotto non è più neppure astrattamente oggetto di *security updates*).

---

[1] Schneier B., *Click here to kill everybody*, Norton (2018)
[2] OECD (2021), *Understanding the digital security of products: an in-depth analysis*: rientra nella definizione di prodotto digitale (*smart product*) qualsiasi prodotto composto da codici e connettibile.
[3] OECD (2021), *Understanding the digital security of products: an in-depth analysis*, cit.
[4] Nel paper dell'OECD si parla di *digital security* piuttosto che di *cyber security* in quanto le problematiche connesse alla vulnerabilità dei prodotti digitali vengono esaminate con un *focus* sugli aspetti socioeconomici piuttosto che su quelli di natura criminale o riguardanti la sicurezza nazionale. Sta di fatto che le vulnerabilità rimangono tali, sia che le si esamini dall'uno o dall'altro punto di vista.
[5] Si calcola che ogni 2.000 linee di codici contengano dalle 20 alle 100 vulnerabilità: quando poi i prodotti digitali sono tra loro interconnessi il numero delle vulnerabilità aumenta esponenzialmente (Dean B., *Strict products liability and the internet of things*, Center for Democracy and Technology, 2018). Per avere un metro di riferimento, basti considerare che un iPhone ha in media 50.000 linee di codici, mentre uno smartphone Android ne ha 12.000.000 circa (*The Economist*, 2017)
[6] È questo il caso dei cd *cyber attacks* volti a prendere il controllo del sistema informatico di un target criptando e rendendo inutilizzabili i dati; ma anche del furto di segreti industriali, di informazioni finanziarie, di dati personali e confidenziali etc. Il tutto si accompagna nella quasi totalità dei casi ad una richiesta di riscatto particolarmente consistente: ma l'esperienza insegna che pur piegandosi al ricatto e pagando spesso non si riottiene la disponibilità dei dati sottratti.

Alert
Innovation & New Technologies

Spesso all'origine della minor sicurezza di un prodotto digitale vi sono ragioni economiche. Per un produttore, ad esempio, può risultare antieconomico destinare delle risorse umane al continuo monitoraggio e aggiornamento di prodotti già commercializzati, anziché indirizzarle allo sviluppo di nuovi prodotti: per non dire di quanto possa essere dispendioso provvedere al richiamo di prodotti successivamente risultati difettosi. In altri casi è il *time-to-market* a condizionare il produttore, e cioè l'esigenza di commercializzare al più presto il nuovo prodotto, per acquistare vantaggi competitivi rispetto ai concorrenti, pur se a dispetto di più approfondite verifiche sulla sicurezza del prodotto: immetti sul mercato presto e se del caso rimedia in un secondo momento. Infine, a volte per confezionare un prodotto più *user-friendly*, si finisce per semplificare e ridurre al massimo i presidi di sicurezza del prodotto.

2. "*All stakeholders should understand digital security risk and how to manage it*": e, proseguendo, "*All stakeholders should take responsibility for the management of digital security risk"*[7]. Questo è il fulcro del problema e dove si dovrebbe intervenire: consapevolezza e responsabilità.

Da un lato gli utenti devono essere informati dei rischi e posti nella condizione di fare scelte consapevoli quando acquistano prodotti digitali; dall'altro lato tutti i soggetti coinvolti nella progettazione, produzione, vendita ed utilizzo di un prodotto digitale devono essere responsabilizzati, ciascuno per quanto di sua competenza.

Occorre quindi anzitutto educare gli utenti: studi di settore evidenziano che ancora oggi vi è scarsa dimestichezza con le tematiche connesse alla *digital security*. Su questo fronte c'è molto da fare: campagne di sensibilizzazione e alfabetizzazione informatica dovrebbero essere in cima alla *to-do list* di ogni Governo. Va da sé, poi, che ogni prodotto digitale immesso sul mercato dovrebbe essere corredato di informazioni comprensibili, accessibili e fruibili anche – se non soprattutto – per un *mainstream user*: veicolare troppe informazioni, magari facendo eccessivo ricorso a terminologia tecnica, può essere controproducente e indurre l'utente a fare un acquisto inconsapevole.

Per altro verso, quanto più un prodotto è complesso, tanto maggiore è – ragionevolmente - il numero di componenti (e di loro *supplier*) coinvolti nella realizzazione del prodotto stesso: con le conseguenti problematiche in tema di allocazione delle responsabilità. La sempre più diffusa sensibilità alla tracciabilità dei prodotti e dei loro componenti è figlia di questa esigenza e della opacità che spesso accompagna la *value-chain*[8] dei prodotti digitali (anche motivata dall'esigenza

[7] OECD (2021), *Enhancing the digital security of products: a policy discussion*: con richiamo rispettivamente a OECD (2015), *Digital security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document* e a OECD (2015), *Recommendation on Digital Security Risk Management*.

[8] In OECD (2021), *Understanding the digital security of products: an in-depth analysis*,cit., si parla di *value-chain* – anziché *supply-chain* – con riferimento alla sequela di coloro che, lungo il processo di realizzazione di un prodotto digitale, apportano uno specifico valore aggiunto per il cliente finale (e che non per forza coincidono con i *supplier*).

di mantenere quanto più possibile "velata", lungo tutta la catena, la sottostante proprietà intellettuale).

3. La sempre maggiore diffusione di prodotti digitali non poteva passare inosservata al legislatore comunitario il quale, in sede di ulteriore armonizzazione dei contratti di vendita[9], ha incluso nell'ambito di applicazione i cd *beni con elementi digitali* [10]. Non si tratta – sia ben inteso - di una disciplina organica dei beni con elementi digitali (che, per convenienza, continueremo a chiamare prodotti digitali), bensì di alcune disposizione che però tengono conto della peculiarità di tali beni con specifico riguardo alla circolazione degli stessi (e con attenzione particolare alla tutela del consumatore).

In base alla richiamata direttiva il venditore di prodotti digitali assicura che al consumatore siano notificati e forniti gli aggiornamenti, compresi gli aggiornamenti della sicurezza, necessari al fine di mantenere la conformità di tali beni (si tratta, si noti bene, di un requisito oggettivo di conformità del bene). La sicurezza digitale diventa quindi uno dei requisiti fondamentali del prodotto digitale. Tuttavia, se tali aggiornamenti non vengono installati dal consumatore entro un termine ragionevole, la responsabilità del venditore per qualsiasi difetto di conformità derivante dal mancato aggiornamento viene meno, sempre che: i) il consumatore sia stato informato della disponibilità dell'aggiornamento e delle conseguenze della mancata installazione, e ii) la mancata o errata installazione dell'aggiornamento non siano dovute a carenze delle istruzioni di installazione fornite al consumatore.

Si bilanciano, in questo modo, i doveri del fornitore/venditore e del consumatore: ed infatti la sicurezza digitale, come si è spiegato, richiede azioni non solo ai vari livelli della *value chain*, ma coinvolge anche l'*end user* al quale pure è richiesta l'ordinaria diligenza nell'utilizzo del prodotto digitale.

Altra disposizione di un qualche interesse, alla luce di quanto fin qui detto, è quella relativa al diritto di regresso. È previsto che quando il venditore di un prodotto digitale è ritenuto responsabile per un difetto di conformità consistente un'azione od omissione (inclusa l'omissione di fornire gli aggiornamenti di cui abbiamo appena trattato) di una persona "*nell'ambito dei passaggi precedenti della catena di transazioni commerciali*", il venditore può agire in regresso nei confronti della persona o delle persone responsabili nella catena.

[9] Direttiva (UE) 2019/771 del Parlamento Europeo e del Consiglio del 20 maggio 2019 relativa a determinati aspetti dei contratti di vendita di beni, in fase di recepimento (il decreto legislativo di attuazione è stato approvato nel corso del Consiglio dei Ministri svoltosi venerdì 29 ottobre 2021). Nella medesima data è stata emanata la Direttiva (UE) 2019/770 relativa alla fornitura di contenuto digitale e di servizi digitali: questa Direttiva non costituisce oggetto di questo breve contributo, ma contiene previsioni analoghe a quelle che si analizzeranno qui appresso.

[10] "*Qualsiasi bene mobile materiale che incorpora o è interconnesso con un contenuto digitale o un servizio digitale in modo tale che la mancanza di detto contenuto digitale o servizio digitale impedirebbe lo svolgimento delle funzioni del bene («beni con elementi digitali»)*": Direttiva (UE) 2019/771, art. 2.5.b).

Alert
Innovation & New Technologies

Al di là della pur scontata azione di regresso nei confronti del produttore, questa previsione apre le porte ad un'azione diretta da parte del venditore (ma non del consumatore, apparentemente) nei confronti di altri soggetti appartenenti alla *supply chain* (se non della *value chain*). Perché ciò sia possibile è necessaria, quindi, un'assoluta trasparenza nei vari passaggi della catena: solo in questo modo si giungerà ad una puntuale allocazione delle responsabilità tra i vari soggetti coinvolti nella realizzazione del prodotto digitale.

4. Per concludere, i prodotti digitali sono parte integrante della nostra vita. La loro pervasività, da un lato, e vulnerabilità, dall'altro lato, impone agli utenti – siano essi *mainstream* o *advanced users* – cautela e consapevolezza nel loro utilizzo. Inoltre, lato *supplier*, è necessario che vengano incentivate *best practice* volte a garantire la sicurezza dei prodotti digitali dal momento della loro immissione in commerciale fino alla loro *end-of-life*. Perché ciò sia possibile occorre massima trasparenza nella *value-chain* e coordinamento tra i vari soggetti coinvolti. La Direttiva (UE) 2019/771 è un punto di partenza: purtroppo è rivolta ad una platea – i consumatori[11] – in massima parte disomogenea rispetto a quella composta da *mainstream users* e *advanced users* di cui si è fin qui parlato: confidiamo che una disciplina organica dei prodotti e della sicurezza digitale possa porre rimedio a questa mancanza.

1.12.2021

Avv. Gianmatteo Nunziante, Partner
E: g.nunziante@nmlex.it
T.: +39 06 695181

Per chiarimenti o informazioni potete contattare l'autore oppure il Vostro Professionista di riferimento all'interno dello Studio

[11] Ai fini della Direttiva (UE) 2019/771 è consumatore "*qualsiasi persona fisica che, in relazione ai contratti oggetto della presente direttiva, agisca per fini che non rientrano nel quadro dell'attività commerciale, industriale, artigianale o professionale di tale persona*".