

10/06/2022

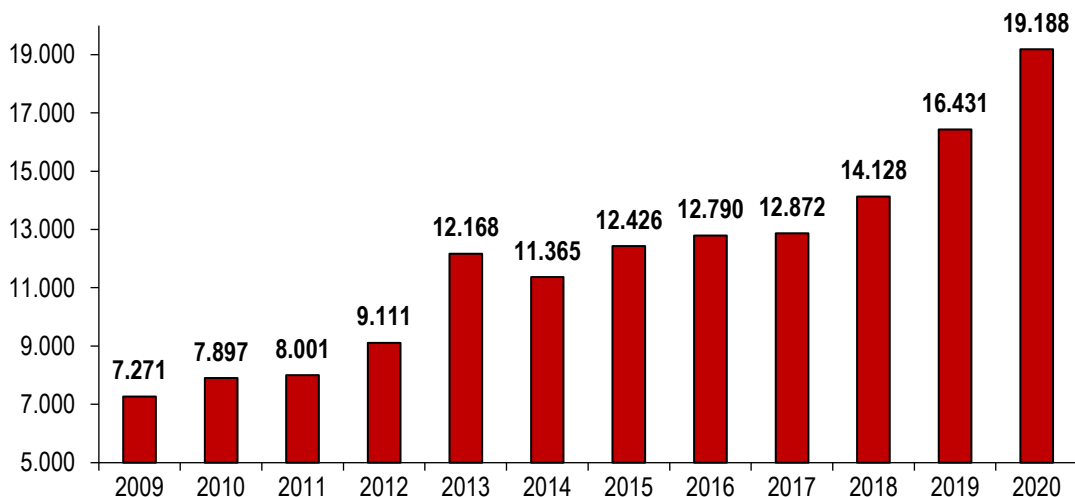
## **Reati informatici +9% all'anno in Emilia-Romagna; ai tempi della *cyberwar* sicurezza informatica cruciale per il 38,1% delle MPI**

Il 2020 è stato un anno di emergenza anche sul fronte della *cybersecurity*, con un aumento tendenziale a doppia cifra dei **reati informatici** (+16,8%) in Emilia-Romagna. Con il diffondersi di strumenti digitali connessi al web, nella nostra vita privata così come sul posto di lavoro, aumenta infatti anche l'esposizione a questo tipo di attacchi.

In un anno in cui i delitti denunciati dalle forze di polizia all'autorità giudiziaria calano complessivamente del -19,0% in Emilia-Romagna e del -17,4% in Italia, le **truffe e frodi informatiche**<sup>1</sup> aumentano del 17,6% raggiungendo le quasi 18 mila denunce all'anno e i **delitti informatici**<sup>2</sup> crescono del 6,8% raggiungendo i 1.345 casi, per una media complessiva di **52 denunce al giorno**.

Nell'ultimo decennio questi **reati informatici** in Emilia-Romagna sono cresciuti al ritmo del 9,3% all'anno. Nel dettaglio, tra il 2015 e il 2020 il totale dei reati informatici è salito del 54,4% con alcune accentuazioni che emergono dall'analisi territoriale: cresce di una volta e mezzo il fenomeno a **Ferrara** (+148,6%) ed è quasi raddoppiato a **Parma** (+96,1%). Si registrano aumenti sopra alla media regionale anche a **Modena** (+68,5%), all'opposto si osserva un dinamismo più contenuto del fenomeno a **Forlì-Cesena** (+23,3%) e **Rimini** (26,5%).

**Denunce di truffe, frodi e delitti informatici in Emilia-Romagna**  
Anni 2009-2020 - delitti denunciati dalle forze di polizia all'autorità giudiziaria



Elaborazione Osservatorio MPI Confartigianato Emilia-Romagna su dati Istat

<sup>1</sup> Truffe su internet al momento di acquisti, Phishing, denaro sottratto durante operazioni bancarie on line (Istat).

<sup>2</sup> Accesso abusivo a sistema informatico/telematico, detenzione/diffusione abusiva di codici di accesso a sistemi informatici/telematici, diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico, danneggiamento di sistemi informatici o telematici (Servizio di Analisi Criminale del Dipartimento della Pubblica Sicurezza).

Sempre più imprese percepiscono la **sicurezza informatica** come un fattore cruciale. Secondo l'ultima indagine Istat sulla situazione e prospettive delle imprese dopo l'emergenza sanitaria oltre due imprese emiliano-romagnole su cinque (il 43,7%) a fine 2021 la ritengono un fattore importante o cruciale, in linea con il dato medio nazionale (43,1%). Anche le micro e piccole imprese (MPI) mostrano una crescente consapevolezza sui rischi della digitalizzazione e dedicano molta attenzione alla sicurezza, in termini di prevenzione di attacchi ed eventuali azioni di recupero dei dati. Come riporta l'indagine Excelsior di Unioncamere-ANPAL, nell'ultimo anno il 38,1% delle MPI che vi investe lo ritiene fondamentale per lo svolgimento della propria attività, con una crescita di 8,6 punti percentuali rispetto al periodo 2016-2020.

L'attuale guerra in Ucraina ha messo in evidenza come uno dei caratteri dei nuovi conflitti ibridi sia quello degli attacchi informatici. Le operazioni di guerra cibernetica comprendono l'attacco a siti istituzionali e non, mettendo in primo piano il tema della sicurezza informatica di enti e imprese. Già nel 2019 (ultimi dati a disposizione) il 9,3% delle piccole imprese italiane – con 10-49 addetti – avevano subito almeno un **incidente di sicurezza ICT**, come l'indisponibilità di servizi ICT, la distruzione o corruzione di dati, o la divulgazione di dati riservati.