Poliziamoderna

25 anni di Postale

1. Lotta al cybercrime Ricorre quest'anno il venticinquennale dalla nascita della Specialità della Polizia di Stato, da quel decreto istitutivo del Servizio polizia postale e delle comunicazioni del 1° marzo 1998 che ne ha disegnato struttura e competenze. Tutelare i servizi postali e delle telecomunicazioni, reprimere i reati contro l'inviolabilità della corrispondenza, sorvegliare l'interno delle sedi e degli impianti appartenenti al ministero delle Poste e delle Comunicazioni, vigilare gli uffici postali, garantire servizi di scorta per le operazioni di trasporto di valori e tutelare il diritto d'autore e delle radiofrequenze: erano queste le principali attività svolte all'inizio dagli operatori per garantire la tutela e la regolarità delle comunicazioni che, in passato, erano basate sulla carta e sulla corrispondenza. Oggi la specificità della Postale è quella di contrastare il cybercrime, una delle principali fonti di allarme per la tenuta del sistema socioeconomico del Paese e delle strutture tecnologiche che ne supportano le funzioni essenziali, che ha attraversato nell'ultimo periodo un ulteriore passaggio evolutivo con l'estensione della minaccia alla pacifica convivenza nelle democrazie moderne anche a livello internazionale. È nella dimensione digitale che le attività produttive, l'approvvigionamento di acqua ed energia, il sistema dei trasporti, gli ospedali, le reti di comunicazione, le pubbliche amministrazioni, gli apparati finanziari, possono subire oggi i danni più consistenti, e le correnti ostilità belliche ne hanno offerto soltanto l'ultima, non necessaria, dimostrazione. La minaccia *cyber* conserva una matrice ancora largamente criminale, se si considera che oltre il 70% degli attacchi cibernetici nel mondo risulta perpetrato per finalità di realizzazione di profitti illeciti ed interroga quindi con forza il ruolo dell'Autorità nazionale di pubblica sicurezza – in chiave di prevenzione dei reati – e, in particolare, l'azione svolta dalla polizia postale e delle comunicazioni, Specialità della Polizia di Stato e principale forza di polizia cibernetica nazionale. In considerazione dello scenario descritto, è possibile affermare che per quanto il fenomeno possa cogliersi all'interno di un prisma di sfaccettature estremamente eterogenee – quali l'attacco ad un sistema informatico che gestisce un servizio pubblico essenziale; il ricorso a tecnologie informatiche per portare frodi su larga scala, sottraendo ingenti patrimoni; lo sfruttamento del mezzo tecnologico per arrivare a colpire persone e bambini nella loro sfera più intima di incolumità e di libertà – esso sottende pur sempre un elemento comune, costituito per l'appunto dalla sua vittima finale: l'uomo. Ne consegue la convinzione che il tema del contrasto alla minaccia cibernetica non possa declinarsi a partire da un approccio settoriale e disarticolato, che rimetta a singoli enti e Istituzioni la risoluzione di singole parti del problema, secondo il loro concreto manifestarsi e in ragione dell'emergenza del momento, ma che occorra piuttosto muovere dalla prospettiva della vittima, per comprendere come la molteplicità vada ridotta ad unità, in un approccio necessariamente olistico che chiami in causa, in primo luogo, i pubblici poteri, alla ricerca di soluzioni armoniche e coordinate. Se l'ambito del *law enforcement* risulta quello maggiormente sollecitato dalla risposta all'allerta *cyber*, va allora adeguatamente sottolineata la bontà della scelta organizzativa compiuta dal nostro Paese, che ha inteso dotarsi di una speciale unità di polizia, a forte vocazione specialistica, in grado di riassumere ed esprimere capacità di contrasto relative a tutte le possibili proiezioni della minaccia cibernetica: la polizia postale e delle comunicazioni. Articolazione specialistica della Polizia di Stato deputata alla prevenzione e al contrasto delle molteplici fenomenologie delittuose commesse sulle reti – e in tal senso espressione più immediata della condivisione di quell'approccio olistico e incentrato sulla persona di cui sopra – la Specialità sta vivendo un processo strategico di rilancio ed evoluzione, tracciato dal Legislatore con la previsione di una Direzione centrale per la polizia scientifica e la sicurezza cibernetica e con il potenziamento delle articolazioni territoriali, per assolvere ai compiti di protezione tanto dei sistemi strategici – di rilevanza nazionale o locale – quanto degli utilizzatori di quei sistemi, ovvero i cittadini, fruitori dei servizi da essi erogati. In questo contesto, l'operato della polizia postale e delle comunicazioni muove lungo due direttrici, una di tipo repressivo e una di natura informativa-preventiva, incentrata sulla capacità di analisi e di allerta precoce finalizzata alla diffusione, in tempo reale, di *alert* di sicurezza riferibili alle minacce in corso a beneficio dell'intero panorama delle infrastrutture informatiche nazionali, a partire da quelle critiche convenzionate con il Centro nazionale anticrimine per la protezione delle infrastrutture critiche (Cnaipic). Il processo in atto, di rafforzamento e rilancio della polizia postale, prevede poi l'istituzione all'interno di ciascuno dei 18 Centri operativi per la sicurezza cibernetica (Cosc) di settori operativi specificamente dedicati da un lato alla protezione delle persone, a partire dai minori, nella proiezione di ogni attività umana nella dimensione cibernetica e quindi delle infrastrutture sensibili anche di rilevanza locale grazie all'istituzione dei Nuclei operativi per la sicurezza cibernetica (Nosc).

Attraverso lo sviluppo e l'implementazione di una nuova piattaforma operativa di *infosharing*, chiamata Sinc3 (Sistema informativo nazionale per il contrasto al cybercrime), il Servizio centrale e i Nosc,

condivideranno in tempo reale informazioni e report di sicurezza in una logica di rete di tipo neurale che consentirà l'immediata disponibilità di dati per assicurare immediato impulso all'azione preventiva e sviluppo all'attività investigativa, a beneficio anche delle realtà strategiche di rilevanza regionale – ivi incluse le Pmi e le pubbliche amministrazioni locali, essenziali nel sistema produttivo del nostro Paese. Questo oramai avviato processo di riorganizzazione, prevede infine il duplice sostegno della formazione del personale e del settore a presidio dell'infrastruttura tecnologica, governata da dirigenti e funzionari del ruolo tecnico. La missione è quella di attivare cicli virtuosi formativi con le accademie del Paese, in grado di riversare nei tre corsi iper specialistici oggi erogati dalla Postale il più attuale *know-how* in tema di sapere tecnologico, ovvero supportare la necessaria ricerca operativa di fronte al continuo mutare degli scenari investigativi. Solo con una rinnovata, elastica capacità di intercettare e reclutare il personale più capace, ovvero di attivare gli strumenti formativi più adeguati, si potrà sostenere la sfida alla convivenza civile lanciata dalla criminalità informatica, per la quale si prevede nel prossimo futuro la capacità di produrre illecitamente 10,5 trilioni di dollari di capitale illegale. *Ivano Gabrielli - direttore del Servizio polizia postale e delle comunicazioni*

2. Verso una nuova Direzione centrale per la sicurezza cibernetica È ormai da tempo sotto gli occhi di tutti come il cybercrime abbia registrato negli ultimi anni un aumento esponenziale, tanto nei numeri quanto nel livello e nella qualità criminale: a livello globale si registrano ogni giorno decine di milioni di attacchi cibernetici, diretti ai sistemi informatici delle infrastrutture critiche (servizi essenziali, pubblica amministrazione, sanità, comunicazione, trasporti e servizi finanziari), verso il sistema delle piccole, medie e grandi imprese, nonché ai danni dei singoli cittadini, con aggressioni che mirano a violarne sia la dimensione della libertà personale che la sfera del patrimonio. I nostri dati, veicolati sulla Rete attraverso gli innumerevoli dispositivi elettronici connessi, rappresentano l'obiettivo più ambito delle organizzazioni criminali, nazionali ed estere, che li utilizzano per minare l'integrità dei servizi pubblici essenziali, realizzare frodi informatiche sempre più sofisticate, dirigere campagne di "cyber-estorsione", alimentare i mercati neri del darkweb e aggredire la sfera più intima della nostra libertà personale, attraverso campagne diffamatorie, atti di persecuzione, di stalking on line, e condotte lesive della libertà sessuale. I minori, al riguardo, sono ancora una volta i soggetti più esposti, vittime di situazioni di cyberbullismo e aggressione psicologica, quando non, purtroppo, delle più odiose condotte di adescamento, violenza sessuale e pedopornografia on line.

Il crimine informatico si conferma dunque una delle principali minacce alla tenuta del sistema economico e sociale del Paese. Appare evidente che la tecnologia, rappresentando una risorsa oramai irrinunciabile per la vita di cittadini, istituzioni ed enti, non permetta più di concepire una compiuta tutela della "sicurezza e ordine pubblico" che non passi anche attraverso la difesa delle dimensioni cibernetiche del nostro vivere quotidiano.

Proprio in una visione politica nazionale sempre più consapevole del rilievo assunto al giorno d'oggi dalla cybersicurezza si inserisce l'istituzione di una Direzione centrale *ad hoc*.

L'architettura nazionale di sicurezza cibernetica è stata strutturata per essere in grado di declinare gli aspetti della cybersicurezza nelle sue diverse posture di competenza di *intelligence*, *defence*, *resilience* e *investigation*, ambito quest'ultimo di appannaggio della Polizia di Stato e della polizia postale e delle comunicazioni in particolare. In tale ambito, il ruolo del ministero dell'Interno assume una posizione centrale che si manifesta primariamente nell'azione di protezione delle reti e delle infrastrutture critiche esercitata dalla polizia postale e delle comunicazioni attraverso il Centro nazionale di protezione delle infrastrutture critiche (Cnaipic), incaricato in via esclusiva della prevenzione e della repressione dei crimini informatici, di matrice comune, organizzata o terroristica, che hanno per obiettivo le infrastrutture informatizzate di natura critica e di rilevanza nazionale del Paese.

La strategicità e l'importanza della materia, hanno determinato una complessiva rivalutazione dell'adeguatezza della dimensione organizzativa del Servizio polizia postale e delle comunicazioni, determinando la scelta, sulla scorta di quanto avvenuto presso altre amministrazioni e in ambito internazionale, del più adeguato livello di Direzione centrale che, come concepita, potrà meglio assolvere ai compiti connessi al ruolo di Autorità generale di contrasto, affidatole dalla normativa europea NIS e dalla normativa sul perimetro di sicurezza nazionale cibernetica.

Particolare attenzione sarà oltretutto data al tema della stessa protezione dell'infrastruttura informatica del ministero dell'Interno, prevedendo alla nascita nell'ambito della nuova Direzione, di un nuovo organismo: il Servizio per la sicurezza cibernetica del ministero dell'Interno, al cui interno opereranno il Cert (*Computer emergency response team*), quale presidio più evoluto per la sicurezza dell'intero comparto ministeriale e il Cv (Centro di valutazione), che assicurerà un'attenta attività di controllo e valutazione sui beni, sistemi e servizi informatici che saranno introdotti e utilizzati all'interno del

predetto dicastero.

Siamo di fronte a una nuova visione della dimensione investigativa nella sua interezza, che rappresenterà un punto di riferimento per tutte le articolazioni della Polizia di Stato in risposta ai segnali di cambiamento e alle nuove istanze di sicurezza per una società sempre più globale e sempre più interconnessa.

Antonio Borrelli - capo della struttura di missione della nuova Direzione centrale

3. Riorganizzazione della polizia postale e delle comunicazioni Lo scorso 21 ottobre, con l'entrata in vigore del decreto del capo della Polizia del 28 giugno 2022, che ha rideterminato l'assetto ordinativo, i compiti, le linee di dipendenza e le dotazioni organiche delle articolazioni territoriali della polizia postale e delle comunicazioni, i Compartimenti e le Sezioni della Specialità si sono trasformati, rispettivamente, in Centri operativi per la sicurezza cibernetica (Cosc) e in Sezioni operative per la sicurezza cibernetica (Sosc), con una rinnovata struttura organizzativa che si inserisce nel più ampio processo di rafforzamento e rilancio della Specialità della Polizia di Stato, chiamata a fronteggiare le sempre crescenti sfide poste dal crimine informatico e dalle tecnologie in costante evoluzione.

La riorganizzazione della ramificata rete territoriale è finalizzata al potenziamento dell'attività operativa nei due settori di più ampia competenza dei reati contro la persona commessi attraverso la rete (a partire dalla tutela dei minori on line) e della protezione degli asset economico strategici.

In ragione dell'estensione geografica e del numero di uffici presenti nelle regioni italiane e per rispondere agli specifici trend criminali delle singole realtà locali, il processo riorganizzativo ha previsto la suddivisione in fasce dei suddetti Centri, per la quale si è anche tenuto conto della dislocazione delle autorità giudiziarie, sedi di Procure distrettuali competenti in materia di cybercrime, e del livello di importanza dei distretti produttivi ed industriali, strategici e quindi sensibili sotto il profilo della tutela della sicurezza cibernetica.

La suddivisione ha comportato il passaggio da 20 Compartimenti regionali a 18 Centri operativi per la sicurezza cibernetica, di cui due con competenza interregionale (Cosc Campania, Basilicata e Molise, e Cosc Piemonte e Valle d'Aosta).

In considerazione della diversa complessità organizzativa delle attività dei Centri, questi sono stati suddivisi in 3 fasce, cui corrispondono tre livelli dirigenziali: in particolare, dei Cosc di "maggiore complessità organizzativa", 6 saranno diretti da dirigenti superiori della Polizia di Stato (Lazio, Campania Basilicata e Molise, Lombardia, Piemonte e Valle d'Aosta, Emilia Romagna, Sicilia Occidentale) e altri 8 da primi dirigenti (Toscana, Veneto, Liguria, Puglia, Calabria, Sicilia Orientale, Sardegna e Friuli Venezia Giulia). Ai restanti 4 Centri operativi (Marche, Umbria, Abruzzo e Trentino Alto Adige) saranno preposti funzionari della qualifica di vice questore aggiunto o vice questore. Inoltre, nelle sedi delle Procure distrettuali sono state previste 9 Sosc (Brescia, Caltanissetta, Campobasso, Catanzaro, L'Aquila, Lecce, Messina, Potenza e Salerno) cui saranno preposti funzionari della Polizia di Stato.

Il processo in atto ha previsto l'istituzione, all'interno di ciascuno dei Centri, di uffici operativi specificamente dedicati alla protezione delle infrastrutture sensibili di rilevanza locale: i Nuclei operativi per la sicurezza cibernetica (Nosc).

L'istituzione dei Nosc, che costituiscono emanazione a livello territoriale del Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche, del quale replicano il modello organizzativo e con il quale operano in stretto raccordo, chiude idealmente un cerchio, completando quel disegno di capillarità e prossimità che consentirà di costituire protezione cibernetica a beneficio dell'intero sistema-Paese, con riguardo sia ai maggiori erogatori dei servizi strategici su scala nazionale, sia degli operatori dei servizi locali, del sistema delle piccole e medie imprese, del sistema delle pubbliche amministrazioni territoriali, attori di un unico sistema partenariale di collaborazione informativa e assistenza operativa.

Ivano Gabrielli

4. A difesa di cittadini e Istituzioni Abbiamo intervistato il dirigente del Centro operativo per la

sicurezza cibernetica “Lazio”, Daniele De Martino, che opera in un territorio particolarmente complesso in considerazione della presenza delle Istituzioni della Capitale d’Italia e della numerosa popolazione della città di Roma.

Quali sono le principali attività di contrasto al cybercrime che la sua struttura operativa affronta quotidianamente? La maggior parte delle denunce e richieste di aiuto riguarda reati diffusi, truffe on line, attivazione di profili *fake*, furto di account, diffamazione. Destano allarme per i danni economici e psicologici alle vittime, le truffe romantiche, le *sextortion* e i falsi siti di *trading on line* e criptovalute. La tutela di minori da aggressioni sessuali, pedopornografia, episodi di cyberbullismo e quella di adulti da minacce gravi e cyberstalking richiedono capacità relazionali, indagini rapide e accurate, immediata presa in carico delle vittime. Di grande impatto i crimini finanziari con violazione dei sistemi informatici in danno di aziende e sistemi bancari; *Man in the middle*, *BEC* e *CEO fraud* sono le truffe più diffuse e in continua evoluzione sono i protocolli criminali tarati sulle vulnerabilità dei sistemi. Il Settore cyberterrorismo riveste rilevanza strategica: acquisisce informazioni utili alla gestione dell’ordine e sicurezza pubblica, di primaria importanza per la Capitale, monitora gruppi eversivi e tratta delicate e rilevanti indagini a tutela delle numerose importanti Istituzioni a Roma. Il Nucleo operativo per la sicurezza cibernetica ha l’impegnativo compito di prevenire e reprimere attacchi informatici in danno di infrastrutture. Solo nell’ultimo anno nel Lazio sono triplicati gli attacchi a sistemi informatici di infrastrutture pubbliche, operatori di servizi essenziali e aziende private, spesso con compromissione dei sistemi informatici.

Che consigli si sente di dare alla popolazione anziana della regione in cui opera il Centro operativo che dirige per difendersi dalle truffe che spesso vengono rivolte nei loro confronti? I truffatori indirizzano le proprie attenzioni malevole nei confronti della popolazione anziana, contando sulla potenziale attenuata attenzione e reattività delle vittime; acquisiscono informazioni private e riservate su vittima e nucleo familiare attraverso accurate ricerche in rete e sfruttando le informazioni postate sui social network; non di rado replicano account, caselle email e numeri di telefono in uso a un congiunto o conoscente della vittima, o a un’istituzione pubblica. Risulta utile un’adeguata informazione indirizzata alle potenziali vittime: una richiesta inconsueta deve allarmare; non utilizzare i link o le utenze fornite dagli attaccanti; non fornire informazioni sensibili e private a interlocutori ignoti; non aprire la porta agli estranei; se riceviamo richieste telefoniche inconsuete, interrompere la conversazione e contattare i propri familiari e/o le forze dell’ordine.

Avete delle attività, soprattutto nel campo della prevenzione, dedicate ai giovani? I nativi digitali vantano abilità e competenze ma spesso non hanno la piena consapevolezza dei rischi connessi all’utilizzo della Rete e dei social network in particolare. Il cyberbullismo, l’adescamento on line e le aggressioni sessuali sono solo parte delle fonti di rischio; nel mondo cyber si incontrano malintenzionati e *sex offender*, si assiste a violenze e abusi, si accede a contenuti sessuali indesiderati, si condividono con superficialità contenuti riservati, si prende parte a iniziative pericolose (diete, anoressia, suicidi, satanismo, challenge, etc), si acquisiscono forme di dipendenza e disordine psicologico e comportamentale. Risulta, pertanto, utilissima un’incisiva attività di prevenzione con campagne e incontri per i giovani, famiglie, educatori e docenti. Nel 2022 gli operatori del Cosc Lazio hanno effettuato incontri con 270 istituti scolastici della Regione, coinvolgendo oltre 42.000 studenti, 1.830 docenti e 2.750 genitori.

Quest’anno si festeggia il venticinquennale della Specialità. Lei è nella polizia postale e delle comunicazioni da tantissimi anni. Può parlarci della sua esperienza personale anche in relazione all’evoluzione che la Specialità ha avuto nel corso del tempo? La polizia postale si occupava di assegni, carte di credito e scorte, telefonia e radiotelevisione e, nel nuovo millennio, ha virato decisamente verso il mondo digitale, prevalentemente crimini finanziari e pedopornografia, acquisendo poi nuove competenze fino alla recente riorganizzazione che ha dato vita alle sezioni minori e social network in un settore, e *financial cybercrime*, Nosc e cyberterrorismo in un altro. Il vero punto di continuità resta la sfida di analizzare costantemente nuovi crimini e nuove modalità di perpetrazione dei reati, aggiornando le forme di contrasto e prevenzione, creando e affinando *best practice*, adeguando i propri assetti organizzativi in relazione alle esigenze in continua evoluzione.

5. Dinamismo lombardo Intervista a Tiziana Liguori, dirigente del Centro operativo per la sicurezza cibernetica “Lombardia”, una regione che vede la presenza di numerose aziende ed imprese operanti sul proprio territorio, molto dinamica e attiva, dove i settori finanziario e terziario assumono carattere predominante.

A chi sono diretti gli attacchi informatici? Gli attacchi informatici, oltre agli obiettivi critici e infrastrutturali, sono diretti prevalentemente verso aziende e imprese. Il cybercrime utilizza tecniche sempre più sofisticate, i target sono più specifici e, in alcuni casi, l’impatto sulle infrastrutture IT è

molto forte. Il loro numero è in continua crescita e va tenuto presente che i dati riportati nelle statistiche sono riferiti ai soli eventi denunciati. In Lombardia, nel 2022, abbiamo registrato oltre 700 casi di attacco, di cui ben 81 episodi di *ransomware*. L'importanza della cybersecurity è purtroppo ancora sottovalutata, spesso accade che un imprenditore assuma consapevolezza dei rischi e delle conseguenze in termini di blocco dell'operatività o reputazione, solo dopo aver subito o sventato un attacco informatico.

Quali sono i principali reati che interessano l'ambito finanziario? Nell'ambito del cosiddetto *financial cybercrime* vi è un incremento degli illeciti legati al fenomeno del trading on line, con numerosi portali presenti sul Web che propongono programmi speculativi, apparentemente redditizi, evidenziando costi di accesso irrisori, ma rendimenti elevati sia nel breve che nel medio termine. Ulteriore tecnica di ingegneria sociale utilizzata dai criminali è il *Man in the middle*: in questo caso il truffatore si inserisce nella corrispondenza elettronica tra due partner commerciali e riesce, sostituendosi ad una delle parti, a farsi accreditare la somma dovuta su un diverso iban bancario. *Phishing*, *smishing*, *vishing* sono, comunque, le frodi più diffuse, volte a manipolare un individuo per ottenere dati riservati e confidenziali, attraverso una mail, un sms o una chiamata vocale. Numerosi sono i percorsi di educazione finanziaria a cui il Cosc partecipa per promuovere la sicurezza nelle operazioni digitali. Altro fenomeno preoccupante è rappresentato dalle *romance scam*, in cui le vittime, frequentando i social network, iniziano una relazione sentimentale virtuale e, nella speranza di incontrare fisicamente la persona "amata", inviano, per le più disparate richieste di aiuto, anche ingenti somme di denaro, spesso destinate all'estero.

Oltre a quelli strettamente connessi all'ambito economico finanziario, quali altri fenomeni criminosi vi impegnano maggiormente, anche in relazione alla complessità del territorio lombardo? Tutti i delitti contro la persona (e in particolare contro i minori) commessi attraverso la Rete. Un ambito di azione assolutamente strategico della polizia postale è rappresentato dal contrasto alla pedopornografia on line, che ci vede impegnati h24 nel monitoraggio della Rete e in attività sotto copertura, in cui risultano essenziali il coordinamento con gli altri Centri operativi – garantito dal Servizio polizia postale e delle comunicazioni – e la cooperazione internazionale. Ci occupiamo inoltre di cyberstalking e di tutti quei crimini informatici afferenti alla sfera sessuale, come ad esempio il *revenge porn* e le estorsioni sessuali. Poiché si tratta di reati che possono avere conseguenze devastanti, sul piano psicologico, per le vittime, credo fermamente nell'importanza della prevenzione. È per questo che, oltre ai tradizionali incontri all'interno delle scuole, organizziamo specifiche iniziative di *cybersecurity awareness* dedicate agli adulti ed ai ragazzi: nel 2022 in Lombardia abbiamo incontrato più di 55.000 adulti e 10.000 ragazzi.

La sua esperienza presso la polizia postale e delle comunicazioni è molto recente, quali sono state le impressioni al primo impatto nell'approdare nella Specialità della Polizia di Stato che si occupa del cybercrime? La Postale, anche in passato, ha sempre stimolato la mia attenzione, in quanto nel giro di pochi anni ha completamente modificato il suo obiettivo istituzionale per soddisfare le nuove esigenze derivanti dall'ingresso nell'era digitale. La vicinanza, inoltre, al mondo giovanile attraverso l'organizzazione di eventi di ampia portata, quali ad esempio *Una vita da social*, unitamente all'assidua presenza di operatori della polizia postale presso luoghi di istruzione e di aggregazione, hanno suscitato in me un forte interesse, facendola ritenere particolarmente "contemporanea". La scelta di passare da un settore altamente specializzato e complesso quale è l'immigrazione, ad un altro ancora più specialistico, non è stata facile, ma oggi posso affermare che le mie aspettative sono state ampiamente soddisfatte, tenuto conto che, grazie all'elevata professionalità degli operatori della polizia postale, è possibile davvero incidere per mitigare l'impatto derivante dalle mutevoli minacce in ambiente *cyber*.

6. Il nuovo logo

Con decreto del capo della Polizia del 31 marzo scorso è stato istituito il nuovo distintivo di specialità per il personale della polizia postale. Abbiamo intervistato l'autrice del progetto grafico, Simona Gallo.

Come si imposta e quali sono i criteri di cui si deve tener conto quando si lavora ad un progetto grafico istituzionale? Quando parliamo del restyling di un marchio dobbiamo rispettare la sua riconoscibilità e dare continuità pur rinnovando la sua immagine. Questo tipo di lavoro richiede un grande rispetto delle regole che sono state imposte dal creativo che ci ha preceduto. Nel caso di un logo istituzionale le regole sono, ovviamente, più rigide e parlando specificamente del logo della Postale è stato imprescindibile mantenere una coerenza grafica con gli scudetti di specialità. È stato un lavoro davvero stimolante. Dovevamo inserire molti concetti, in uno spazio relativamente piccolo. Quando mi è stato proposto di lavorare a un progetto così importante, ho accettato con la convinzione che si sarebbe trattato di un'esperienza unica.

Quali sono i nuovi temi grafici nuovi e qual è il loro significato? Cercavamo un nuovo logo che rappresentasse la modernità e allo stesso tempo mantenesse un tono istituzionale. Abbiamo lavorato sul “naming” cambiando il nome da polizia delle telecomunicazioni a polizia postale. Abbiamo reso la “trombetta con le ali” più lineare e moderna ridisegnandola e adattandola al nuovo stile grafico e abbiamo inserito il tricolore nell’ala della chiocciola. Infine, volevamo rappresentare le interconnessioni della rete Internet e la presenza sul territorio nazionale dei centri operativi della Postale e il loro collegamento con la sede operativa centrale. Da qui la creazione della rete posta sul fondo che collega le strutture territoriali e rappresenta parallelamente le interconnessioni informatiche. Abbiamo mantenuto i colori originali data l’importanza della riconoscibilità e la coerenza grafica con lo scudetto di specialità precedente.

Il suo logo accompagnerà il lavoro degli operatori della Postale... Per un grafico, ogni progetto è un piccolo figlio nato da riflessioni, spunti e metodo. Sono soddisfatta del risultato e piacevolmente emozionata all’idea di vederlo applicato. Stiamo vivendo un’importante accelerazione dello sviluppo digitale e questa realtà digitale ci espone tutti a continui rischi, spesso non percepibili. Sia come donna sia come mamma, mi sento molto vicina al lavoro degli operatori della Postale che si trovano sempre più di fronte a nuove e più complesse sfide investigative. È stato un onore collaborare con loro e altrettanto lo sarà accompagnarli, nel mio piccolo, nella loro quotidianità.

03/05/2023