**Tavola Rotonda UILFPL L'Aquila**

# "La Pubblica Amministrazione nel mirino dell'hacker:

# prevenzione e gestione a tutela di cittadini e lavoratori"

**28 giugno 2023 ore 10.00**

Sede Ance L'Aquila

**Intervento del Segretario Generale UILFPL**

**Domenico Proietti**

## ATTACCHI HACKER CONTRO LA PUBBLICA AMMINISTRAZIONE

Innanzitutto, vorrei ringraziare la dottoressa Spera per la professionalità e l'autorevolezza con cui sta conducendo questa tavola rotonda. Rivolgo un caloroso saluto a tutti voi.

Ho colto in maniera molto gradita l'invito di Antonio perché questo è un tema di cui si parla ancora molto poco e che, invece, il sindacato, e segnatamente la UIL FPL, fa bene a porre al centro dell'attenzione. Rivolgo poi un saluto al nostro segretario regionale Alfiero Antonio Di Giammartino.

In autunno faremo un'iniziativa nazionale su questo tema. Costruiremo un evento nazionale nel quale chiameremo al confronto alcune delle persone oggi intervenute, coinvolgendo anche le istituzioni a livello governativo.

In Abruzzo avete vissuto un'esperienza molto drammatica, ma le risposte avute all'interno della vostra pubblica amministrazione sono state esemplari, a dimostrazione dell'alta professionalità delle lavoratrici e dei lavoratori che operano in questo settore.

Questo, per noi, è un valore fondamentale sul quale far leva. Veniamo da anni nei quali la PA è stata rappresentata in maniera sbagliata, per responsabilità di qualche sciocco. Li chiamavano i furbetti del cartellino, ma in realtà sono i cretinetti del cartellino. Per colpa di qualche cretinetto è stata fatta di tutta l'erba un fascio all'interno della PA, non valorizzando, invece, le grandi professionalità che ci sono. Ma questo ha generato anche una percezione negativa della PA, al punto che la stessa politica ha iniziato a penalizzare i lavoratori pubblici.

Noi abbiamo fatto un'iniziativa, lo scorso febbraio, su questo tema, di cui voglio richiamare solo alcuni punti. Quello più importante, e che, fortunatamente, ha avuto esito positivo in questi giorni, è stato il differimento del trattamento di fine rapporto

dei lavoratori pubblici, che andava da due anni fino, addirittura, a sette anni, se si andava in pensione con quota 100.

Questa cosa è andata avanti dal 2011, ma grazie anche alla battaglia portata avanti dalla UIL e dalla UIL FPL siamo arrivati, l'altro ieri, alla decisione della Corte costituzionale che ha sancito l'incostituzionalità di quella norma.

Noi lo abbiamo sempre sottolineato con molta forza: il tfr è salario differito. Lo Stato ha operato una vera e propria appropriazione indebita dei soldi dei lavoratori; e oggi chiediamo al Governo e al Parlamento di attuare la sentenza della Corte costituzionale, ridando il tfr in tempi certi a 1.600.000 lavoratori del settore pubblico, che in questi anni si sono visti sottrarre 14 miliardi di euro.

Ma la penalizzazione nel settore pubblico non ha riguardato solo questo punto, ma anche, per esempio, il trattamento di malattia, che ha un regolamento separato tra pubblico e privato, con penalizzazione del primo. Così come ha riguardato anche la tassazione della contrattazione di secondo livello. Nel settore privato c'è un'aliquota del 10%, che scende fino al 5%, mentre nel pubblico c'è l'aliquota massima.

Bisogna invertire questa tendenza, occorre smetterla di penalizzare il lavoro pubblico, e il primo risultato ottenuto sul tfr ci conforta nel continuare questa battaglia. Noi speriamo che già dalla prossima legge di bilancio ci sia un'inversione di tendenza sostanziale che rimetta i lavoratori pubblici al centro dell'azione.

Il lavoro pubblico, come avete dimostrato anche voi, è fondamentale non solo per rispondere a questo tipo di problema, ma anche per dare valore a quelli che sono i servizi pubblici che andrebbero forniti.

**I NUMERI DEGLI ATTACCHI HACKER E COME FUNZIONANO**

A darci un'idea della portata del fenomeno è la relazione annuale al Parlamento sulle attività svolte dall'Agenzia per la cybersicurezza nazionale (ACN), che analizza il periodo che va dal 1° gennaio al 31 dicembre del 2022, la quale mette in luce come l'anno appena passato sia stato particolarmente denso di attività malevole ai danni di settori governativi e di infrastrutture critiche. L'Italia è risultata essere tra i Paesi maggiormente colpiti da virus e attacchi cibernetici specifici, con un particolare accanimento verso il settore sanitario e quello energetico.

Parlando in numeri, nel 2022 si sono verificati 1.094 cyber attacchi, con una media di circa 90 al mese. Di questi, 126 hanno avuto conseguenze certificate dalle stesse

vittime, per una media di 10,5 incidenti al mese, mentre 160 sono stati rivolti verso istituzioni pubbliche e 57 hanno avuto un impatto confermati dai soggetti stessi che ne sono stati colpiti. Essi hanno causato un malfunzionamento dei sistemi e conseguenti ritardi nell'erogazione dei servizi.

Qui in Abruzzo avete avuto un'esperienza molto drammatica in tema di cyberattacchi, ma le risposte avute all'interno della vostra pubblica amministrazione sono state esemplari, a dimostrazione dell'alta professionalità delle lavoratrici e dei lavoratori che operano in questo settore.

Questo, per noi, è un valore fondamentale sul quale far leva. Veniamo da anni nei quali la PA è stata rappresentata in maniera sbagliata, per responsabilità di qualche sciocco. Li chiamavano i furbetti del cartellino, ma in realtà sono i cretinetti del cartellino. Per colpa di qualche cretinetto è stata fatta di tutta l'erba un fascio all'interno della PA, non valorizzando, invece, le grandi professionalità che ci sono. Ma questo ha generato anche una percezione negativa della PA, al punto che la stessa politica ha iniziato a penalizzare i lavoratori pubblici.

Sono, poi, diversi i modi con cui i criminali informatici riescono a sottrarre informazioni importanti e dati personali agli ignari che cadono nella loro trappola. Si va dalle mail contenenti allegati in diversi formati, i quali, una volta aperti, consentono al virus di entrare all'interno del dispositivo utilizzato e di infettarlo, ai messaggi di posta elettronica ed sms contenenti dei link che inducono il lettore ad aprirli tramite falsi allarmi e messaggi ingannevoli. Questi emulano comunicazioni provenienti da banche, da poste italiane e da importanti istituzioni e avvisano i destinatari di azioni urgenti da compiere (aprendo, per l'appunto, documenti o cliccando i link proposti) per evitare di incorrere in problemi di varia natura.

I rischi che si corrono sono ovviamente di natura economica. Gli hacker riescono ad entrare nei conti correnti e a trasferirne il contenuto; oppure fanno attivare alla vittima inconsapevole un abbonamento che sottrae denaro poco alla volta, molte volte senza che questi se ne accorga. E ancora, rubano documenti e dati molto importanti che saranno riconsegnati solo dietro il pagamento di un ingente riscatto.

Altre volte, poi, le stesse piattaforme social, quali Instagram e Facebook, costituiscono un veicolo attraverso cui gli hacker riescono a mettere in atto furti d'identità e, una volta entrati nei profili dei soggetti colpiti, iniziano a scrivere messaggi

compromettenti per la reputazione della vittima ai diversi contatti, chiedendo poi un riscatto; oppure li indirizzano verso altre truffe di vario genere.

In base a quanto detto, dunque, non ci stupiamo nel vedere come i numeri degli attacchi informatici ai danni delle pubbliche amministrazioni continuino a crescere. Stiamo parlando di un comparto caratterizzato da una mole di burocrazia eccessiva, spesso con procedure lunghe e complesse e, soprattutto, con sistemi informatici ormai ritenuti obsoleti. Considerando che l'età media degli impiegati nel settore pubblico si attesta intorno ai 50 anni, è facile immaginare un livello di alfabetizzazione informatica molto basso. Ragion per cui, professionisti del settore, abituati a penetrare nei sistemi di difesa più sicuri, anche solo per diletto o "per sfida", non trovano alcun problema nel violare i sistemi pubblici.

Si sa che poi, tanto maggiore è il danno causabile, tanto più sarà la possibilità di creare irrequietezza ed incertezza nelle vittime ed avere successo nella propria intenzione criminosa. E quale miglior destinatario di una pubblica amministrazione che ogni giorno si trova a doversi occupare di pratiche di estrema importanza non solo per il funzionamento di tutto l'apparato statale in sé, ma anche per imprese e cittadini, come nel caso di gare di appalti, concessioni edilizie, servizi inerenti agli istituti scolastici?

Lo scopo è, chiaramente, quello di paralizzare le attività e di rubare dati per poi chiedere un riscatto, dietro la minaccia di vendita degli stessi sul dark web, ovvero il mercato nero digitale.

**LE CONTROMISURE MESSE IN ATTO**

Dunque, se è vero che gli attacchi contro le pubbliche amministrazioni sono aumentati negli ultimi tempi, è anche vero che si è cominciato a mettere in atto delle strategie difensive per eludere i cyber attacchi.

Innanzitutto, importante è stata l'introduzione, con regolamento n. 679/2016, del GDPR, ovvero il regolamento generale sulla protezione dei dati, che all'art. 33 dispone che: "*il titolare del trattamento* (ossia il Comune, e, in qualità di legale rappresentante, il Sindaco), *deve notificare la violazione all'autorità di controllo competente (vv. art. 55) senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e per le libertà delle persone fisiche"*, con ciò stabilendo

un'importante rete di comunicazione tra i soggetti coinvolti e l'autorità di controllo, per tenere traccia ed analizzare gli incidenti verificatisi.

È stato, poi, introdotto con decreto-legge n. 105/2019 il Perimetro Nazionale di Sicurezza Cibernetica con lo scopo di assicurare un elevato livello di sicurezza delle reti e dei sistemi informatici di alcune pubbliche amministrazioni e di aziende private opportunamente individuate. Questa normativa coinvolge solamente alcuni soggetti che svolgono una funzione ritenuta essenziale per l'interesse pubblico in settori particolarmente sensibili, come quelli della difesa, delle telecomunicazioni, dei sistemi bancari, di quelli finanziari e dei trasporti.

I soggetti che vi rientrano devono adottare requisiti procedurali e di sicurezza più stringenti rispetto a chi ne resta fuori, attraverso il censimento di beni, dati ed informazioni che potrebbero essere oggetto di attività criminosa, così da poter adottare le adeguate contromisure.

Fondamentale è stata, poi, l'istituzione dell'Agenzia per la cybersicurezza nazionale, con decreto-legge 82/2021, che ha il compito di tutelare la sicurezza e gli interessi nazionali nel campo della cybersicurezza e ad attuare la Strategia Nazionale di Cybersicurezza, volta a pianificare, coordinare e attuare misure tese a rendere il Paese più sicuro, attraverso il raggiungimento di 82 misure entro il 2026.

Inoltre, non va dimenticato che il PNRR ha stanziato importanti risorse, pari a 623 milioni di euro per l'implementazione della cybersicurezza.

È necessario, dunque, che tutte le risorse citate siano utilizzate per aumentare il grado di sicurezza dei nostri sistemi informatici e che ogni struttura pubblica si doti di strumenti di difesa che tengano conto della complessità e multidimensionalità del fenomeno; ma è altrettanto essenziale agire tempestivamente attraverso un'opera di prevenzione attuando un'adeguata formazione degli operatori. Più i dipendenti saranno formati ed informati dei possibili rischi, più alta sarà la possibilità di scongiurare il problema. È necessario, inoltre, che l'educazione contro i rischi informatici sia promossa a tutti i livelli, anche a livello scolastico, così che le nuove generazioni siano istruite fin da subito per contrastare truffe e raggiri.

E lo dobbiamo fare consapevoli anche di un disegno più complessivo, che riguarda, in particolare, il settore della sanità. Noi veniamo da tre anni di pandemia, che hanno messo in evidenza molte problematiche. Innanzitutto, oggi, nel nostro Paese, si è dimostrato che la miglior politica economica è una buona politica sanitaria. Se il nostro

SSN, pur indebolito dai tagli che ci sono stati negli ultimi dieci anni, non avesse retto l'urto della pandemia, il nostro Paese non avrebbe avuto, nel 2021 e nel 2022, una crescita del Pil rispettivamente del 6% e del 4%, a dimostrazione che ogni risorsa destinata alla sanità migliora le prestazioni ed ha un riverbero positivo su tutto il sistema economico e produttivo del Paese.

Allora dobbiamo chiedere al Governo che bisogna incrementare il Fondo del SSN, il quale, invece, sia nell'ultima legge di bilancio che nel DEF di aprile, va in direzione opposta. Questo lo riteniamo assolutamente sbagliato. E lo abbiamo fatto presente anche in occasione dell'ultimo incontro avuto con il ministro Schillaci. Bisogna destinare più risorse alla sanità proprio perché siamo convinti delle affermazioni fatte prima.

Al momento non vediamo risposte, ma solo impegni generici. Noi pensiamo, invece, che si debba andare concretamente a prevedere una destinazione di risorse adeguate.

E affermiamo anche che in questi tre anni sono stati fatti degli errori drammatici, il più rilevante dei quali è stato quello di non aver utilizzato le risorse del Mes sanitario, che si sostanziavano in 35 miliardi di euro restituibili in tantissimi anni ad un tasso di interesse bassissimo. La maggior parte dei partiti ha agitato bandierine ideologiche paventando che, se si fossero utilizzati le risorse del Mes sanitario, si sarebbe messa in discussione l'autonomia dello Stato italiano. Ma non c'è niente di più sbagliato, sono solo fandonie, dato che la Commissione Europea ha più volte messo per iscritto che le risorse del Mes sanitario erano fuori dagli interventi salvastato, come era stato, invece, in Grecia. Quindi, non c'era alcun rischio, ma solo una miopia della classe politica che non ha voluto utilizzare quelle risorse. Quelle risorse erano fondamentali perché tutti gli studi ci dicono che per riallineare la spesa italiana alla media europea occorrono 10 miliardi all'anno per i prossimi 5 anni. Si tratta di una mole di risorse imponente di cui il nostro Paese, attualmente, non dispone.

Ciononostante, noi pensiamo che si debba continuare su questa strada e, a tal proposito, abbiamo indicato come UIL e UIL FPL ai partiti, di maggioranza e di opposizione, la strada per reperire risorse aggiuntive. La principale è quella della tassa sugli extraprofitti. Durante la pandemia e con la guerra in Ucraina ci sono state aziende che hanno fatto extraprofitti straordinari. Facendo una tassa sugli extraprofitti, il governo Draghi aveva stimato che si potevano incassare 10 miliardi all'anno per i prossimi 3 anni. L'attuale governo ha derubricato questo tema e prevede un incasso di poco più di 1 miliardo. È sbagliato. Noi non siamo per un fisco che opprime le

aziende. Siamo, però, per un fisco equo. In un momento di emergenza come questo, chi ha fatto extraprofitti è giusto che paghi qualcosa in più rispetto agli altri.

Un'altra strada è quella della lotta all'evasione fiscale. Il governo sta discutendo una delega fiscale in Parlamento che non parte da quello che noi riteniamo necessario, ovvero una svolta epocale contro l'evasione fiscale. Ogni anno il governo si autocertifica oltre 100 miliardi di evasione. Per questo, dovremmo darci l'obiettivo di recuperare almeno 30 miliardi ogni anno incrociando le banche dati.

La mobilitazione svolta nel mese di maggio, di cui, a tal proposito, ringraziamo la UIL FPL Abruzzo per la partecipazione, ha avuto come effetto che il governo riaprisse i tavoli con i sindacati. Ci siamo incontrati il 30 di maggio con la presidente Meloni e ci stiamo incontrando in questi giorni con i vari ministri. Però lo abbiamo detto anche ieri al ministro Calderone in occasione del tavolo sulle pensioni: avere conquistato il tavolo è importante, ma per il sindacato il tavolo è uno strumento, non un fine. Noi vogliamo che da quei tavoli vengano risposte ai problemi delle persone che rappresentiamo e, se non ci saranno risposte, noi continueremo la mobilitazione affinché queste risposte arrivino. Compito del sindacato, e della UIL in particolare, non è quello di far nascere o di far cadere il Governo. La UIL non ha mai avuto governi amici o nemici. Per la UIL ci sono sempre stati i governi della Repubblica. Noi abbiamo giudicato i governi in base alle cose che facevano. Quando facevano cose buone lo riconoscevamo e quando facevano cose negative lo abbiamo sottolineato e ci siamo mobilitati.

Questa è la prospettiva con la quale ci apprestiamo al confronto che speriamo possa continuare in maniera unitaria con CISL e CGIL, perché quello che abbiamo fatto in questi mesi è frutto di un rinnovato confronto unitario.

In ultimo, lo abbiamo ripetuto sia al ministro Zangrillo sia al ministro Schillaci, bisogna continuare con la contrattazione. Noi abbiamo a fatica rinnovato il contratto nel 2022, dopo dieci anni di blocco della contrattazione, con risvolti molto importanti sulle buste paga dei lavoratori. Adesso, però, non possiamo stare fermi. Bisogna che il governo metta le risorse necessarie a rinnovare il contratto, già scaduto, 2022-2024. Questo sarà uno degli obiettivi sui quali lavoreremo nelle prossime settimane e incalzeremo il governo affinché arrivino risposte all'altezza dei problemi posti.