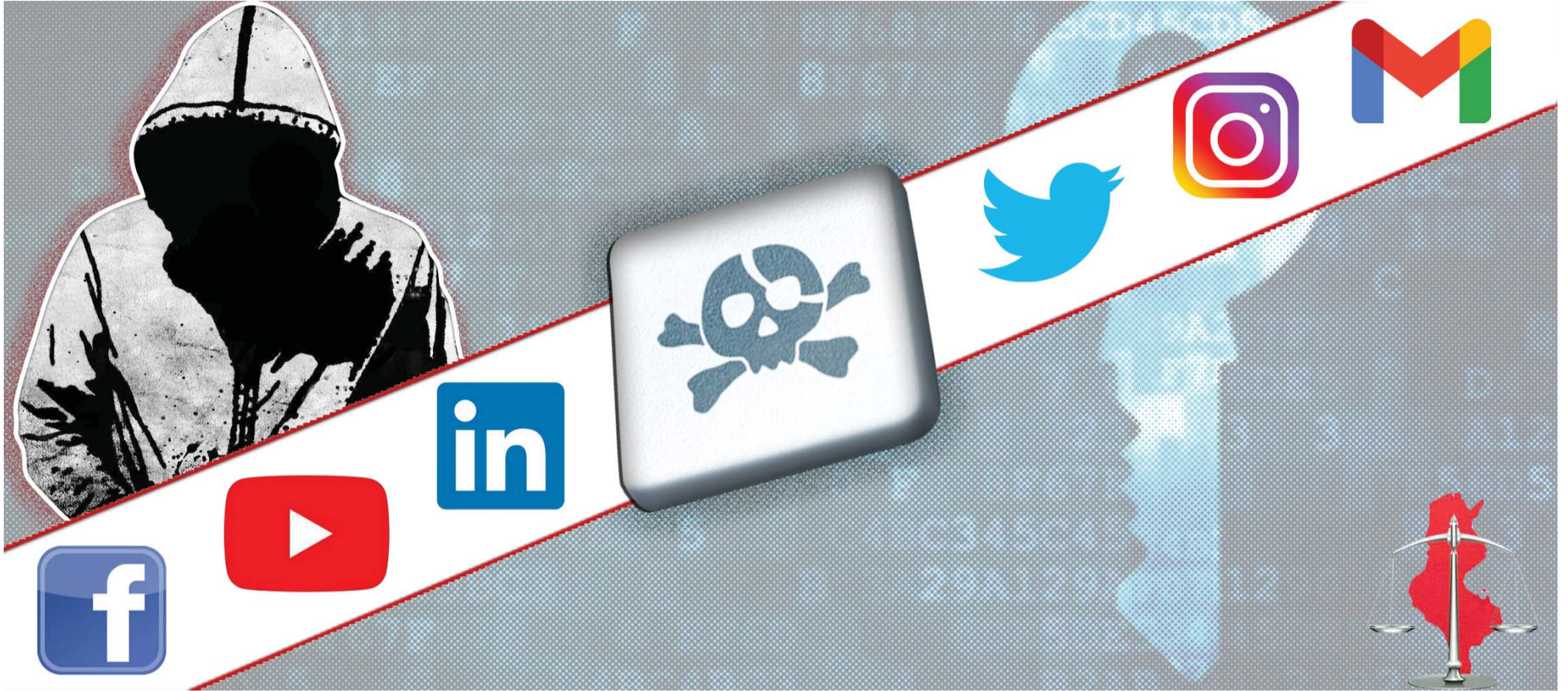


# تونس تخوض حربا مفتوحة ضد الجرائم الإلكترونية

## غياب قوانين تعاقب على الجرائم السيبرانية أدى إلى ارتفاع نسق عمليات التصيد والاختراق



عدو مجهول

وفي مايو 2018، صادقت الحكومة على مشروع قانون مكافحة الجرائم المتعلقة بأنظمة المعلومات والاتصال، وينص الفصل الأول من مشروع هذا القانون، على أنه يهدف إلى "التوقي من جرائم أنظمة المعلومات والاتصال وزجرها وضبط الأحكام الخاصة بجمع الأدلة الإلكترونية". لكن لم يقع تبنيه بعد من قبل البرلمان.

ويؤكد الخبراء والمتابعون أنه في ظل ضعف القوانين، تتضرر الشركات بشكل متواتر من عمليات القرصنة المتكررة.



وأشار هيثم المير مدير عام شركة كيبستون المختصة في أمن المعلومات في حديثه لـ "العرب" إلى أن شركات تونسسية (خاصة أو عمومية) تلقت خسائر فادحة جراء هذه الجرائم. ولاحظ أن "الهجمات الأعنف والخسائر الأقوى كانت مع بداية من 2020". مرجحا تواصل عمليات الاختراق.

وفي ظل تواضع الأداء الحكومي، وجدت الشركات نفسها في عزلة ودون مساندة حكومية حتى تتمكن من مواجهة القرصنة بشكل فعال.

ويرر ارتفاع هذه الظاهرة بغياب أطر تنظيمية وتشريعية ناجعة إضافة إلى نقص الكفاءات المختصة في هذا المجال، مع تفضيل الغالبية منهم العروض المغربية في الخارج، إضافة إلى ضعف الإلمام والوعي بعملية القرصنة وخطورتها.

ويراي المير فإن الحل لا يكمن في الاحتفاء بشراء برامج للتصدي للفيروسات والاختراقات، بل يجب التعامل مع الجريمة الإلكترونية وفق خطة إستراتيجية وليس كمجرد عطل فني.

وفيما كانت تونس سباقا ومن أوائل الدول التي أنشأت وكالة مختصة لسلامة المعلومات سنة 2002، إلا أن جهودها تلاشت اليوم وباتت تنحصر في مركزا ضعيفا في هذا المجال في ظل ضعف الإمكانيات والإجراءات، وهو ما تدفع لفته الشركات على لأحثة الدول الحامية للمعطيات الشخصية.

أولويات الحكومة حسب استنتاجات المتابعين لأشغالها في معالجة الأوضاع الاقتصادية والاجتماعية المتردية، في الوقت الذي تعرض فيه الجرائم الإلكترونية أمنها للخطر. وأوضح شوقي قداس رئيس الهيئة الوطنية لحماية المعطيات الشخصية لـ "العرب" أنه "هناك تجاهل لخطورة الجرائم الإلكترونية في تونس رغم ارتفاعها محليا ودوليا".

وأشار إلى أن الهيئة قامت بعمليات تحسيسية وتثقيفية للتحذير من مخاطر القرصنة، وقامت بحملة للتخفيف على تجنب استعمال فيس بوك وأغلقت صفحاتها الرسمية حيث يحذو الناس حذوها. ويراي قداس فإن مثل هذه الخطوات ضرورية لحماية أمن البيانات الشخصية من جهة والأمن القومي من جهة ثانية.

وأشار إلى أن الهيئة أرادت أن تقول إنه لديها موقف واضح من مواقع التواصل وتدعو التونسيين للحد من استعمال وسائل تواصل مضمونة ووطنية. وشرح بالقول "طلبنا من وزارة التكنولوجيا أن تحت بعض الشركات الناشئة على تطوير تطبيقات وطنية تضمن فرصة التواصل والوصول إلى المعلومات بشكل آمن".

وعلى رغم الجهود للتوعية بأهمية حماية المعلومات والبيانات الشخصية، إلا أن قداس يشير إلى تقصير حكومي وعدم تحمل المسؤولية في التصدي لهذه الظاهرة خاصة في ظل التراخي في إصدار قوانين للمعاقبة على مثل هذه الجرائم.

ويقول قداس "لا يوجد قانون يعاقب فيه على الجرائم السيبرانية في تونس".

### ضعف القوانين

رغم أن تونس أقرت في أكتوبر عام 2019 الاستراتيجية الوطنية للأمن السيبراني بهدف تعزيز خط الدفاع التكنولوجي والرقمي، إلا أنه لحد الآن لم تسن الحكومة قانونا يحد من الجرائم الإلكترونية.

ووقعت تونس في السابق على اتفاقيات إقليمية ودولية، من بينها اتفاقية مجلس أوروبا، لحماية المعطيات الشخصية، كما أنها تملك قوانين تضبط التعامل مع هذا النوع من البيانات أثناء المعاملات التجارية، إلا أن البرلمان لم يصادق إلى الآن على مشروع القانون الأساسي المتعلق بحماية المعطيات الشخصية الذي وقع اقتراحه منذ عام 2018.

ولطالما أبدت أوساط سياسية واقتصادية وحقوقية استغرابها من تجاهل هذا القانون الذي يمكن من قانون صارم لحماية المعطيات الشخصية في البلاد، كما سيسمح بإدراج تونس على لأحثة الدول الحامية للمعطيات الشخصية.

القرصان باستهداف نظامها المعلوماتي. وتشرح أنه في مرحلة أخرى وفي ما يتعلق بالبرمجيات الخبيثة فإن القرصان يقوم أولا بتفسير جميع المعطيات الموجودة بالجهاز سواء كان حاسوبا أو غيره، ثم في مرحلة لاحقة يحاول القرصان الدخول في اتصال مع الضحية ويطلب فدية عادة ما تكون مبالغ مالية كبيرة بالعملة الافتراضية "بيتكوين" أو الدولار، ويذم أنه يتلقى الفدية المطلوبة سيقوم بموافاة الضحية برمز التشفير ويسترجع معطياته.

ومع الارتفاع المخيف لنسق عمليات القرصنة، دعت الوكالة الوطنية للأمن السيبرانية إلى الرفع من درجة الحذر واليقظة، وذلك خاصة لدى المسؤولين عن سلامة النظم المعلوماتية والموظفين العاملين بمختلف الهياكل والمؤسسات الوطنية، وذلك أولا بعدم فتح أي رابط أو ملف مصاحب يرد عبر البريد الإلكتروني إلا بعد التثبت من مصداقيته وسلامته وعدم احتوائه على برمجيات خبيثة. وأكدت الوكالة على ضرورة اجتناب الدخول في اتصالات مع القرصان وعلى ضرورة رفض دفع الفدية المطلوبة وعدم الوثوق فيه باعتباره شخصا مارقا عن القانون.

وأشارت إلى ضرورة أن يتم تخزين المعطيات بصفة دورية ومنظمة وأن تتم عملية التخزين على أقراص صلبة خارجية أو غيرها، كما تؤكد الوكالة على ضرورة توفر مخططات استمرار العمل ومخططات استئناف العمل بالنسبة لجميع المؤسسات لضمان الاستمرارية في حال وقوع حادث سيبراني أو اختراق معلوماتي.

وتستنتج الوسلاطي أن وجود الخطر بنسبة صفر في المئة في مجال السلامة المعلوماتية أمر محال ولا وجود له في أي دولة من دول العالم، مهما كان تقدمها في مجال السلامة المعلوماتية.

وفيما يجمع الخبراء والمتابعون على أن الجرائم الإلكترونية تترك جميع دول العالم القوية والضعيفة على حد سواء، إلا أن التقصير الحكومي في التصدي إلى هذه الظاهرة يبدو جليا في تونس.

ويؤكد الخبراء على ضرورة التعامل باكثر جدية مع عمليات القرصنة، إلا أن ضعف الوعي بخطورة التهديدات السيبرانية فاقم من هذه الظاهرة، التي لا تبدو من

الاعتداءات التي تمس الحياة الخاصة للأفراد وتهدد الأمن والسيادة الوطنيين. وشهد هذا النوع من الجرائم ارتفاعا ملحوظا في تونس في زمن الجائحة وقبله، وتحديدا في السنوات العشر الأخيرة التي أعقبت ثورة يناير بسبب تداعيات فترة الانتقال الديمقراطي الصعب على الأمن القومي.

وكتشفت آمال الوسلاطي المستشارة الإعلامية لـ "الوكالة الوطنية للسلامة المعلوماتية" في حديثها لـ "العرب" أن محاولات الاختراق والهجمات السيبرانية شهدت ارتفاعا خلال السنوات 2019 و2020 وبداية 2021 وذلك بنسبة تتجاوز 30 في المئة. وأوضحت الوسلاطي أن القرصنة ركزوا محاولاتهم لاختراق النظم المعلوماتية والمواقع خلال السنوات الأخيرة عبر استعمال تقنية التصيد والبرمجيات الخبيثة، حيث يقوم القرصان بإرسال رسائل إلكترونية تحتوي على روابط وملفات مصاحبة تتضمن برمجيات خبيثة وذلك عبر البريد الإلكتروني.

وبمجرد أن يقوم المتلقي بفتح الرابط أو الملف المصاحب الذي يحتوي على البرمجيات الخبيثة، يصاب الجهاز الذي هو بصدد استغلاله وتنتشر الإصابة والعدوى في صفوف أجهزة زملائه في المؤسسة، التي قام

بمحاولات الاختراق والهجمات السيبرانية شهدت ارتفاعا خلال السنوات 2019 و2020 وبداية 2021، وذلك بنسبة تتجاوز 30 في المئة



تزيد الجرائم الإلكترونية، التي شهدت ارتفاعا مقلقا في تونس خلال الأونة الأخيرة، من أعباء الحكومة التي باتت مطالبة ببذل المزيد من الجهود لحماية أمنها السيبراني مع تعرض المؤسسات الحكومية والحسابات الشخصية لاختراقات متواترة من قبل القرصنة عبر استعمالهم تقنية التصيد والبرمجيات الخبيثة. ويؤكد الخبراء أن القرصنة باتت بمثابة «حرب يومية» في البلاد وتشكل تحديا وخطرا حقيقيا، خاصة مع غياب قوانين صارمة تعاقب على هذا النوع من الجرائم.

وإذ لم توافق الضحية على إرسال المال، تتلقى تهديدا بنشر صورها ومحادثاتنا الشخصية.

وحددت الشرطة 75 متضررا من ضحايا المتهم من مختلف ولايات (محافظات) البلاد.

ولا يتوقف سجل الجرائم الإلكترونية على ذلك، حيث سبق للبريد التونسي أن تعرض لعملية تصيد إلكتروني نتجت عنها خسائر مالية لأصحاب الحسابات البريدية، كما راج مؤخرا تعرض بنك تونس لمحاولة اختراق.

وأقر نوفل فريخة مدير الوكالة الوطنية للسلامة المعلوماتية في تصريحات لوسائل إعلام محلية أن بلاده "في حرب مفتوحة مع المخترقين وأن القرصنة أصبحت حربا يومية مع تونس لمحاولات اختراق".

وتضاعف هجمات حجب الخدمة، مشيرا إلى "تطور طرق الهجمات الإلكترونية والاختراقات التي يمكن أن تمس المعطيات الشخصية والبنكية وغيره"، لافتا إلى أن "نوعية الهجمات تطورت ويوجد كل يوم سلاح جديد في هذه الحرب مما يستوجب يقظة وحماية كاملة".

ويطرح ارتفاع الجريمة الإلكترونية تحديا أمام الحكومة التونسية، كسائر دول العالم التي تتربص بها تهديدات سيبرانية عابرة للحدود خاصة في أوقات الأزمات الطارئة.

وشكلت القيود التي فرضتها الجائحة والتي استنوجت اللجوء والاستفادة من خدمات الفضاء الرقمي، اختيارا للحكومات حيث باتت مطالبة بالحفاظ على مستوى كاف من الأمن السيبراني للعمل عن بُعد، وضمان عدم تعرض وسائل التواصل للقرصنة والتوقف.

ويتعلق الأمن السيبراني بحماية المواقع والحسابات من الاختراق الذي ينفذه قرصنة سواء كانوا أشخاصا أو مجموعات بهدف سرقة المعلومات والبيانات أو السطو على الحسابات المصرفية أو لتعطيل عمل موقع ما أو للتحكم فيه.

أمنة جبران صحافية تونسية

تونس - سجلت الجرائم الإلكترونية ارتفاعا مقلقا في تونس في الأونة الأخيرة، مع تعرض حسابات مؤسسات حكومية وشخصية إلى الاختراق والقرصنة.

وزادت الهجمات السيبرانية بشكل لافت أعقاب ظهور الجائحة، حيث استغل القرصنة "الهاكرز" انشغال الحكومة بالتصدي لانتشار الوباء، لزيادة أنشطتهم غير القانونية واستخدامهم غير المشروع للوسائل التكنولوجية والرقمية بهدف التشنويع على عمل المواقع الرسمية وتصيد البيانات الشخصية مقابل الحصول على أموال.

وفيما وجد التونسيون في الفضاء الرقمي وسيلتهم للعمل والدراسة والترفيه أثناء فترة الحجر الصحي، خاصة موقع فيس بوك الذي يلاقي رواجاً لدى الأوساط الشبابية مع بلوغ عدد مستخدميه نحو 7.4 مليون مستخدم حسب إحصائيات محلية، إلا أن الانفصاح الواسع على الإنترنت والفضاء السيبراني، رافقته تعديات وأنشطة إجرامية.

وتعرض موقع التلفزيون الرسمي التونسي الأسبوع الماضي، إلى عملية اختراق، حيث تم تعطيل الصفحة الرسمية للتلفزيون، وموقع الفنانين الأولى والثانية. وبحسب إذاعة محلية، تمت عملية الاختراق من قبل "الذئب المغربي".

وفي فبراير الماضي، أعلنت وزارة الداخلية التونسية أنها ألقت القبض على شخص بتهمة قرصنة أكثر من سبعين حسابا في موقع التواصل الاجتماعي فيس بوك وابتزاز أصحابها وتلقي أموال بناء على ذلك.

وحسب بيان الوزارة الذي نشر على موقعها الرسمي، فقد فتحت الشرطة تحقيقا في قضية تهديد وابتزاز بعد شكوى سيدة قالت إنها تعرضت لقرصنة حسابها في فيس بوك من قبل مجهول.

وتمكنت الشرطة من إلقاء القبض على المشتبه به وهو تونسي يبلغ من العمر 34 سنة، وحسب البيان فإنه محل تفتيش لفائدة وحدات أمنية مختلفة من أجل التحليل والابتزاز والإساءة إلى الغير عبر شبكات التواصل.

وقال البيان إن المتهم اعترف بقرصنة عدة حسابات فيس بوك، ومقايضة أصحابها بمبالغ مالية مقابل إرجاعها،