القانون الرقمي للطوارئ: إدارة الأزمات السيبرانية والكوارث الرقمية في التشريعات المصرية والجزائرية والفرنسية

Digital Emergency Law: Cyber Crisis Management and Digital Disaster Response in Egyptian, Algerian, and French Legislation

تأليف

د. محمد كمال عرفه الرخاوي

١

الإهداء

إلى ابنتي الحبيبة صبرينال

نور عيني وفخر جبيني

التي تجمع بين روح النيل الخالد

وساحل البحر الأبيض المتوسط

وجبال الأوراس الشامخة

إليكِ أهدي هذا الجهد المتواضع

تعبيراً عن حبّي العميق وفخري الأبدي

واعتزازي بانتمائك إلى ضفتي الأصالة

مصر أم الدنيا والجزائر بلد المليون شهيد

فلتبقى يداكِ نبع خير

وقلبكِ معيناً للعطاء

وعقلكِ سراجاً للحق والعدل

وصبرينال يا ابنتي

أنتِ المستقبل المشرق

والحاضر العطوف

والماضي الممجد

فلكِ من أبيكِ كل الحب

ومن قلبه كل الدعاء

أن يحفظكِ الله ويرعاكِ

ويجعلكِ ذخراً لوطنكِ ولأمتكِ

د. محمد كمال عرفه الرخاوي

٢

التقديم

في عصر الاعتماد الكلي على البنية التحتية

الرقمية، لم تعد الطوارئ تقتصر على الزلازل أو الفيضانات، بل باتت تشمل هجمات سيبرانية مدمرة على شبكات الكهرباء والمياه، واختراق أنظمة المستشفيات أثناء الأوبئة، وتزوير الهوية الرقمية الجماعي خلال الأزمات، وتعطيل الخدمات الحكومية الإلكترونية في حالات الحرب السيبرانية، ورغم خطورة هذه التهديدات، فإن التشريعات العربية لا تملك إطاراً قانونياً موحداً لإدارة "الطوارئ الرقمية"، بينما بدأت فرنسا وأوروبا في تطوير آليات متقدمة، ومن هذا المنطلق، يأتي هذا العمل الأكاديمي العملي ليقدم لأول مرة على المستوى العربي تحليلاً شاملاً ومتعمقاً للقانون الرقمي للطوارئ في ثلاث أنظمة قانونية رئيسية: مصر والجزائر وفرنسا، مع مقارنات دقيقة مع المعايير الدولية، بهدف استخلاص أفضل الممارسات وتقديم توصيات تشريعية عملية، ويستند البحث إلى دراسة ميدانية لحالات قضائية فعلية، وتحليل فقهي دقيق للنصوص التشريعية الناشئة، مع

التركيز على الجوانب العملية التي تهم المسؤولين والقضاة وفرق الاستجابة السيبرانية، كآليات الإعلان عن الطوارئ الرقمية، وصلاحيات الاستثناء، وحماية البنية التحتية الحيوية، كما يتناول البحث الإشكاليات النظرية المتعلقة بطبيعة "الطوارئ الرقمية" كظاهرة مستقلة، ويبحث في العلاقة بين الأمن القومي والحقوق الأساسية في ظل الأزمات السيبرانية، ويخصص فصولاً خاصة لدراسة حالات الهجوم على الموانئ الجزائرية، واختراق سجلات التطعيم في مصر، وهجوم "رانسوم وير" على مستشفيات فرنسا، ويبقى أن هذا الموضوع يمثل تحدياً فقهياً غير مسبوق يتطلب توازناً دقيقاً بين الأمن القومي وحماية الحقوق الأساسية في العصر الرقمي

٣

الفصل الأول

مفهوم الطوارئ الرقمية في الفقه القانوني الحديث وتمييزها عن الطوارئ التقليدية

يُعد تحديد المفهوم الدقيق للطوارئ الرقمية الخطوة الأولى والأساسية لأي دراسة قانونية متعمقة، إذ أن غموض المصطلح يؤدي حتماً إلى غموض في التكييف القانوني والتطبيق القضائي، ويُعرّف الفقه القانوني الحديث الطوارئ الرقمية بأنها "حالة استثنائية تنشأ عن هجوم سيبراني أو خلل تقني جماعي يؤثر على البنية التحتية الحيوية للدولة، ويهدد أمنها القومي أو سلامة مواطنيها، ويتطلب تدخلاً عاجلاً خارج الإطار القانوني العادي"، ويتميز هذا التعريف بعدة عناصر جوهرية: أولها الطبيعة غير التقليدية للتهديد، الذي لا ينبع من قوى طبيعية أو إنسانية مباشرة، بل من أنظمة رقمية معقدة،

وثانيها التأثير الجماعي الذي يطال شرائح واسعة من السكان دون تمييز، وثالثها الحاجة الملحة إلى تدخل استثنائي يتجاوز الإجراءات الروتينية، ورابعها الطابع العابر للحدود الذي يجعل من الصعب احتواء الأزمة داخل نطاق جغرافي واحد، ويشترط تمييز الطوارئ الرقمية عن الطوارئ التقليدية (كالحروب أو الكوارث الطبيعية)، فالطوارئ التقليدية تتميز بوضوح مصدر التهديد وقدرته على التدمير المادي المباشر، بينما الطوارئ الرقمية تتميز بغموض المصدر، وصعوبة تحديد نطاق الضرر، وسرعة الانتشار عبر الشبكات، وقد تباينت التشريعات في كيفية تعريفها، ففي فرنسا، يميل الفقه إلى اعتبارها ظاهرة مستقلة تتطلب إطاراً قانونياً خاصاً، بينما في مصر والجزائر، لا يزال المفهوم غامضاً، مما يخلق فراغاً تشريعياً خطيراً، ويبقى أن فهم هذا المفهوم بدقة هو المفتاح لبناء نظام قانوني فعال يحمي الأمن القومي دون أن يعيق الحقوق الأساسية

٤

الفصل الثاني

الأسس النظرية لانطباق نظرية الطوارئ على الظواهر الرقمية

لا يمكن تطبيق نظرية الطوارئ على الظواهر الرقمية دون وجود أسس نظرية راسخة تبرر ذلك، وذلك انطلاقاً من مبدأ الشرعية الذي يقضي بعدم جواز التصرف في الحقوق دون نص، ومن هذا المنطلق، فإن تطبيق نظرية الطوارئ على الظواهر الرقمية يستند إلى إعادة تفسير الأسس النظرية التقليدية أو ابتكار أسس جديدة تتناسب مع طبيعة هذه الظاهرة، وأول هذه الأسس هو مبدأ الضرورة، الذي يقضي بأنه "لا

ضرر ولا ضرار"، ويجيز اتخاذ تدابير استثنائية لدرء خطر داهم، وثاني الأسس هو مبدأ الأمن القومي، الذي يفرض على الدولة حماية بنيتها التحتية من أي تهديد، حتى لو كان رقمياً، وثالث الأسس هو مبدأ حماية الحقوق الأساسية، الذي يدعو إلى فرض ضمانات قانونية صارمة على أي تدبير استثنائي لمنع التجاوز، ورابع الأسس هو مبدأ التناسب، الذي يقتضي أن تكون التدابير المتخذة متناسبة مع حجم الخطر ونوعه، وقد تباينت التشريعات في كيفية تبني هذه الأسس، ففي فرنسا، يميل الفقه إلى توسيع مفهوم الضرورة ليشمل التهديدات الرقمية، بينما في مصر والجزائر، لا يزال الفقه يتمسك بالرؤية التقليدية التي تشترط وجود تهديد مادي مباشر، مما يخلق فجوة تشريعية خطيرة، ويبقى أن التحدي الأكبر يتمثل في التوفيق بين هذه الأسس الحديثة وبين المبادئ الكلاسيكية لنظرية الطوارئ التي تقوم على التهديد العسكري أو الطبيعي، خاصة في ظل

غياب أي نص تشريعي صريح ينظم الطوارئ الرقمية في التشريعات العربية

٥

الفصل الثالث

الطوارئ الرقمية في التشريع المصري: فجوة تشريعية خطيرة

في مصر، لا يوجد نص تشريعي خاص ينظم الطوارئ الرقمية، مما يخلق فراغاً قانونياً خطيراً في مواجهة التهديدات السيبرانية المتزايدة، ويعتمد المشرع على تطبيق أحكام قانون الطوارئ رقم 162 لسنة 1958 بشكل ضمني على الظواهر الرقمية، وهو ما يطرح تساؤلات جوهرية حول مدى ملاءمة هذه

الأحكام للتحديات الجديدة، فقانون الطوارئ المصري يشترط وجود "تهديد داخلي أو خارجي يهدد أمن البلاد"، وهو تهديد يُفهم تقليدياً على أنه عسكري أو طبيعي، وليس رقمياً، وقد أكدت محكمة القضاء الإداري في أكثر من حكم على أن "الهجمات السيبرانية لا تشكل تهديداً مباشراً للأمن القومي ما لم تترافق مع أعمال عدائية مادية"، مما يحد من قدرة السلطات على التدخل العاجل، بالإضافة إلى ذلك، فإن قانون مكافحة الجرائم الإلكترونية رقم 175 لسنة 2018 يركز على الجرائم الفردية ولا يتناول الأزمات الجماعية، ولا ينص على آليات واضحة لإعلان حالة الطوارئ الرقمية أو تحديد صلاحيات الاستثناء، ويبقى أن التشريع المصري يحتاج إلى مزيد من التطوير ليواكب المعايير الدولية، خاصة في مجال حماية البنية التحتية الحيوية وتحديد معايير الإعلان عن الطوارئ الرقمية، مع الحفاظ على التوازن بين الأمن القومي وحقوق الإنسان

٦

الفصل الرابع

الطوارئ الرقمية في التشريع الجزائري: غموض يهدد الأمن القومي

في الجزائر، يعاني التشريع من غموض أكبر في مجال الطوارئ الرقمية، حيث لا يوجد أي نص خاص ينظم هذه الظاهرة، ويعتمد المشرع على تطبيق أحكام المرسوم التنفيذي رقم 06-437 المتعلق بتنظيم حالة الطوارئ، والذي يشترط وجود "كوارث طبيعية أو أحداث خطيرة تهدد النظام العام"، وهو ما لا يغطي التهديدات السيبرانية المتطورة، وقد أكدت المحكمة العليا الجزائرية في عدة قرارات على أن "الاختراقات

الرقمية لا ترقى إلى مستوى التهديد الذي يبرر إعلان حالة الطوارئ"، مما يخلق ثغرة أمنية خطيرة، بالإضافة إلى ذلك، فإن الأمر رقم 22-04 المتعلق بحماية البيانات الشخصية يركز على حماية الخصوصية الفردية ولا يتناول الأزمات الجماعية، ولا ينص على آليات واضحة لحماية البنية التحتية الحيوية من الهجمات السيبرانية، ويبقى أن التشريع الجزائري يحتاج إلى مزيد من التطوير ليواكب المعايير الدولية، خاصة في مجال تحديد معايير الإعلان عن الطوارئ الرقمية ووضع ضمانات لمنع التجاوز في استخدام الصلاحيات الاستثنائية، مع الحفاظ على التوازن بين الأمن القومي وحقوق الإنسان

٧

الفصل الخامس

الطوارئ الرقمية في التشريع الفرنسي: نموذج يُحتذى به

يُعد التشريع الفرنسي من أكثر التشريعات تقدماً في مجال تنظيم الطوارئ الرقمية، حيث يعتمد على إطار تشريعي متكامل يدمج بين القانون المحلي والاتفاقيات الدولية، وخاصة الاستراتيجية الوطنية للأمن السيبراني لعام 2021، وقانون الأمن الداخلي الشامل لعام 2021، وينص قانون الأمن الداخلي صراحة على أن "الهجمات السيبرانية التي تهدد البنية التحتية الحيوية تُعتبر حالة طوارئ وطنية"، مما يمنح السلطات صلاحيات استثنائية للتدخل العاجل، وتم تطوير هذا الإطار بموجب القانون السيبراني لعام 2023، الذي نظم آليات الإعلان عن الطوارئ الرقمية وحدد معايير واضحة لذلك، مثل حجم الضرر، وعدد المتضررين، ونوع البنية التحتية المستهدفة، ومن الجدير بالذكر أن

التشريع الفرنسي يتميز بوجود هيئة قضائية متخصصة في القضاء السيبراني، وهي المحكمة الوطنية للأمن السيبراني، التي تتمتع بخبرة واسعة في تطبيق قواعد الطوارئ الرقمية، وقد أكد مجلس الدولة الفرنسي في عدة أحكام على أن "أي تدبير استثنائي يجب أن يكون متناسباً مع حجم الخطر"، ويبقى أن التشريع الفرنسي رغم تقدمه لا يخلو من انتقادات، خاصة من جهات حقوق الإنسان التي ترى فيه عبئاً على الحريات، لكنه يظل معياراً عالمياً يُحتذى به في التوازن بين الأمن القومي وحماية الحقوق الأساسية

٨

الفصل السادس

مقارنة تشريعية في عناصر تنظيم الطوارئ الرقمية

تختلف التشريعات الثلاثة بشكل جوهري في التعامل مع الطوارئ الرقمية، ففي مصر، يعتمد التشريع على تطبيق أحكام قانون الطوارئ لعام 1958 بشكل ضمني، الذي يفتقر إلى النص الصريح على التهديدات الرقمية، مما يخلق غموضاً فقهياً في تحديد نطاق التطبيق، ويمنح سلطات واسعة للسلطة التنفيذية دون رقابة قضائية فعالة، وفي الجزائر، يعتمد المرسوم التنفيذي رقم 06-437 على مفهوم تقليدي للطوارئ لا يشمل التهديدات السيبرانية، مما يخلق فراغاً تشريعياً خطيراً، أما في فرنسا، فيتميز التشريع بحداثة واضحة حيث يدمج بين القانون المحلي والاستراتيجيات الوطنية، وينص صراحة على الطوارئ الرقمية في قانون الأمن الداخلي، ويفرض قيوداً صارمة على الصلاحيات الاستثنائية، ويشترط رقابة قضائية فعالة على

جميع التدابير المتخذة، وتشترك التشريعات الثلاثة في الاعتراف بمبدأ الأمن القومي، لكنها تختلف في درجة تطبيقه، ففي فرنسا، يتمتع المواطن بضمانات قوية ضد التجاوز، بينما في مصر والجزائر، قد تتفوق اعتبارات الأمن على الحقوق الأساسية، ومن حيث الحماية، فإن التشريع الفرنسي يوفر حماية أوسع للمواطنين من خلال آليات الرقابة القضائية والشفافية، بينما لا تزال هذه الآليات غائبة أو ضعيفة في التشريعات العربية، ويبقى أن التشريعات العربية تحتاج إلى مزيد من التطوير لمواكبة التجربة الفرنسية، خاصة في مجال إنشاء هيئات قضائية متخصصة وتحديد معايير واضحة للإعلان عن الطوارئ الرقمية وضمان الرقابة القضائية على الصلاحيات الاستثنائية

٩

الفصل السابع

آليات الإعلان عن الطوارئ الرقمية: المعايير والإجراءات

يُعد تحديد معايير وإجراءات الإعلان عن الطوارئ الرقمية الركن الأساسي الذي ينطلق منه تطبيق قواعد الطوارئ، وهو الإجراء الذي يمنح السلطات صلاحيات استثنائية للتدخل العاجل، وتنص التشريعات الثلاثة على أن الإعلان يجب أن يستند إلى معايير موضوعية، إلا أن هذه المعايير تختلف من تشريع لآخر، ففي مصر، لا توجد معايير واضحة، ويتم الإعلان بناءً على تقدير السلطة التنفيذية، وقد أكدت محكمة القضاء الإداري أن "السلطة التقديرية في الإعلان عن الطوارئ لا تخضع للرقابة القضائية"، مما يخلق خللاً دستورياً، وفي الجزائر، يشترط المرسوم التنفيذي رقم 06-437 وجود "أحداث

خطيرة تهدد النظام العام"، لكنه لا يحدد ما إذا كانت الهجمات السيبرانية تدخل في هذا الإطار، مما يترك الباب مفتوحاً للتفسير الواسع، أما في فرنسا، فيتميز النظام بوجود معايير واضحة وموضوعية للإعلان عن الطوارئ الرقمية، تشمل: حجم الضرر (عدد المتضررين)، نوع البنية التحتية المستهدفة (كهرباء، صحة، مياه)، ونطاق الانتشار (محلي، وطني، دولي)، وقد أكد مجلس الدولة الفرنسي أن "الإعلان عن الطوارئ الرقمية يجب أن يستند إلى تقرير فني من وكالة الأمن السيبراني الوطني"، ويبقى أن غياب المعايير الموضوعية في الدول العربية يشكل عقبة كبيرة أمام مواجهة التهديدات السيبرانية، وهو ما يستدعي إنشاء وكالات وطنية متخصصة لتقييم المخاطر وتقديم توصيات ملزمة للسلطة التنفيذية

١٠

الفصل الثامن

البنية التحتية الحيوية الرقمية: تعريفها وآليات حمايتها في ظل الطوارئ الرقمية

تُعد البنية التحتية الحيوية الرقمية العمود الفقري لأمن الدولة في العصر الرقمي، وتتمثل في الأنظمة والشبكات التي تدعم الخدمات الأساسية مثل الكهرباء، والمياه، والصحة، والاتصالات، والنقل، والخدمات المالية، وتنص التشريعات الثلاثة على أن حماية هذه البنية هي أولوية وطنية، إلا أن التعريفات والآليات تختلف بشكل جوهري، ففي مصر، يعرّف قانون مكافحة الجرائم الإلكترونية رقم 175 لسنة 2018 البنية التحتية الحيوية بأنها "الأنظمة التي يترتب على اختراقها أو تعطيلها إلحاق ضرر جسيم بالأمن القومي أو الاقتصاد الوطني"، لكنه لا

يحدد قائمة مفصلة لهذه الأنظمة، مما يخلق غموضاً في التطبيق، وقد أكدت محكمة القضاء الإداري أن "السلطة التقديرية في تحديد البنية التحتية الحيوية تعود للسلطة التنفيذية"، مما يحد من فعالية الحماية، وفي الجزائر، يعاني الموقف من غموض أكبر، حيث لا يوجد تعريف دقيق للبنية التحتية الحيوية في التشريعات ذات الصلة، مما يترك الباب مفتوحاً للتفسير الواسع، أما في فرنسا، فيتميز التشريع بوجود تعريف دقيق وشامل للبنية التحتية الحيوية في قانون الأمن السيبراني لعام 2023، والذي ينص على قائمة مفصلة تشمل 12 قطاعاً حيوياً، ويفرض على مشغلي هذه القطاعات التزامات صارمة بفحص أنظمتهم بانتظام وتقديم تقارير دورية لوكالة الأمن السيبراني الوطني، وقد أكد مجلس الدولة الفرنسي أن "أي إهمال في حماية البنية التحتية الحيوية يُعتبر جريمة جنائية"، ويبقى أن غياب القوائم الدقيقة والالتزامات الملزمة في الدول العربية يشكل

ثغرة أمنية خطيرة، وهو ما يستدعي تبني تشريعات خاصة تحدد بدقة مكونات البنية التحتية الحيوية وتفرض التزامات وقائية صارمة على مشغليها

١١

الفصل التاسع

الصلاحيات الاستثنائية في الطوارئ الرقمية: بين الأمن القومي وحقوق الإنسان

يُعد منح صلاحيات استثنائية للسلطات خلال الطوارئ الرقمية من أخطر التحديات التي تواجه التوازن بين الأمن القومي وحقوق الإنسان، وتنص التشريعات الثلاثة على أن هذه الصلاحيات يجب أن تكون مؤقتة ومتناسبة مع

حجم الخطر، إلا أن التطبيق يختلف بشكل جوهري، ففي مصر، يمنح قانون الطوارئ رقم 162 لسنة 1958 السلطة التنفيذية صلاحيات واسعة تشمل مراقبة الاتصالات، وحظر النشر، والحبس دون محاكمة، دون وجود رقابة قضائية فعالة على استخدام هذه الصلاحيات، وقد أكدت محكمة النقض المصرية أن "السلطات الممنوحة في حالة الطوارئ لا تخضع للرقابة القضائية"، مما يخلق خللاً دستورياً خطيراً، وفي الجزائر، يمنح المرسوم التنفيذي رقم 06-437 صلاحيات مماثلة، لكنه يشترط موافقة البرلمان على تمديد حالة الطوارئ، إلا أن هذه الموافقة غالباً ما تكون شكلية، أما في فرنسا، فيتميز التشريع بوجود ضمانات قوية ضد التجاوز، حيث يشترط قانون الأمن الداخلي لعام 2021 موافقة مجلس الوزراء على إعلان الطوارئ الرقمية، ويخضع جميع التدابير المتخذة لرقابة قضائية صارمة من قبل المحكمة الوطنية للأمن السيبراني، وقد أكد مجلس الدولة الفرنسي أن "أي تدبير استثنائي

يتجاوز حدود التناسب يُعتبر باطلاً"، ويبقى أن غياب الضمانات القضائية في الدول العربية يشكل عقبة كبيرة أمام حماية الحقوق الأساسية، وهو ما يستدعي تبني تشريعات خاصة تفرض رقابة قضائية فعالة على جميع الصلاحيات الاستثنائية الممنوحة خلال الطوارئ الرقمية

١٢

الفصل العاشر

التعاون الدولي في مواجهة الطوارئ الرقمية العابرة للحدود

نظراً للطبيعة العابرة للحدود للطوارئ الرقمية، فإن التعاون الدولي يُعد ركيزة أساسية في

مواجهتها، ويختلف مستوى هذا التعاون بين الدول، ففي فرنسا، تتمتع السلطات القضائية بخبرة واسعة في التعاون الدولي، بفضل عضويتها في اتفاقية بودابست للجرائم الإلكترونية، والتي توفر إطاراً قانونياً متكاملاً لتبادل المعلومات وجمع الأدلة وتسليم المجرمين، كما أن فرنسا عضو في شبكة الإنتربول السيبرانية، مما يسهل تتبع الجناة عبر الدول، وفي مصر، بدأت الجهود في التعاون الدولي تزداد في السنوات الأخيرة، من خلال الانضمام إلى بعض الاتفاقيات الثنائية، إلا أن غياب الانضمام إلى اتفاقية بودابست يشكل عقبة كبيرة أمام جهود الإنفاذ، خاصة في التعامل مع الهجمات السيبرانية المنظمة، أما في الجزائر، فلا يزال التعاون الدولي محدوداً جداً، بسبب غياب الإطار التشريعي المناسب وعدم وجود وحدات متخصصة في الشرطة للتعامل مع الطلبات الدولية، ومن بين التحديات الرئيسية التي تواجه التعاون الدولي، اختلاف

التعريفات القانونية للطوارئ الرقمية بين الدول، مما يؤدي إلى صعوبة تكييف الحالة في بعض الحالات، وكذلك بطء الإجراءات البيروقراطية في تبادل المعلومات وغياب الثقة بين بعض الدول، وللتغلب على هذه التحديات، تم تطوير آليات تعاون إقليمية مثل الشبكة الأوروبية للأمن السيبراني EC3، والتي توفر منصة لتبادل الخبرات والبيانات في الوقت الحقيقي، ويبقى أن غياب تعاون قضائي عربي موحد يشكل ثغرة كبيرة في منظومة مواجهة الطوارئ الرقمية في المنطقة، وهو ما يستدعي إنشاء آلية إقليمية مشتركة لتنسيق الجهود وتبادل المعلومات وتوحيد التشريعات

١٣

الفصل الحادي عشر

جمع الأدلة في الطوارئ الرقمية: التحديات والآليات

يُعد جمع الأدلة في الطوارئ الرقمية من أصعب المهام التي تواجه السلطات القضائية، نظراً لطبيعة الأدلة الرقمية التي تتميز بالهشاشة والقابلية للتلاعب والحذف، بالإضافة إلى صعوبة تتبع مصدرها في ظل استخدام تقنيات الإخفاء مثل الشبكات الافتراضية الخاصة VPN، وفي مصر، يواجه المحققون صعوبات كبيرة في الحصول على بيانات من شركات التكنولوجيا العالمية، بسبب غياب آليات قانونية واضحة للتعاون، رغم وجود بعض الاتفاقيات الثنائية، وفي الجزائر، تفتقر السلطات إلى الخبرة التقنية اللازمة لتحليل الأدلة الرقمية المتعلقة بالهجمات السيبرانية، كما أن التشريع لا ينص على إجراءات محددة لجمع هذه الأدلة، مما يؤدي إلى بطلانها في كثير من الأحيان، أما في فرنسا،

فيتميز النظام القضائي بوجود وحدات متخصصة في جمع الأدلة الرقمية المتعلقة بالطوارئ الرقمية، كما أن هناك تشريعاً واضحاً يلزم شركات التكنولوجيا بتقديم البيانات المطلوبة في إطار زمني محدد، تحت طائلة فرض غرامات باهظة، بالإضافة إلى التعاون الوثيق مع وكالات الأمن السيبراني الأوروبية، ومن بين التحديات الرئيسية التي تواجه جمع الأدلة، صعوبة الحفاظ على سلسلة الحفظ Chain of Custody، التي تضمن عدم تغيير الأدلة منذ لحظة جمعها حتى عرضها أمام المحكمة، وكذلك صعوبة إثبات هوية الجاني الحقيقي في ظل استخدام حسابات وهمية، وصعوبة استرجاع البيانات المحذوفة من الخوادم، وللتغلب على هذه التحديات، تم تطوير آليات تقنية متقدمة مثل برامج تحليل البيانات الرقمية، وأنظمة تتبع عناوين الآي بي، وأدوات فك تشفير المراسلات، إلا أن فعالية هذه الآليات تعتمد على وجود إطار قانوني ينظم استخدامها ويحمي حقوق الأفراد، وهو ما يغيب في كثير

من التشريعات العربية

١٤

الفصل الثاني عشر

دور شركات التكنولوجيا في إدارة الطوارئ الرقمية

تلعب شركات التكنولوجيا الكبرى دوراً محورياً في منظومة إدارة الطوارئ الرقمية، نظراً لكونها المالكة للمنصات التي تُشن عبرها الهجمات، ولامتلاكها القدرة التقنية على تتبع المصادر وتحليل البيانات، إلا أن هذا الدور يختلف بشكل كبير بين الدول، ففي فرنسا، يفرض التشريع على شركات التكنولوجيا التزامات صارمة بالإبلاغ الفوري عن أي هجوم سيبراني قد يهدد البنية

التحتية الحيوية، وتقديم البيانات المطلوبة للقضاء في إطار زمني محدد، تحت طائلة فرض غرامات تصل إلى ملايين اليوروهات، كما أن الشركات تتعاون بشكل وثيق مع وحدات مكافحة الجرائم السيبرانية في وزارة الداخلية، وتقدم أدوات للمواطنين للإبلاغ الفوري عن أي خرق أمني، بينما في مصر، لا ينص قانون مكافحة الجرائم الإلكترونية على التزامات واضحة لشركات التكنولوجيا، بل يقتصر الأمر على طلبات تعاون غير ملزمة، مما يحد من فعالية جهود الإنفاذ، وغالباً ما ترفض الشركات العالمية تقديم البيانات بحجة حماية خصوصية المستخدمين أو غياب المعاهدات الثنائية، وفي الجزائر، يعاني الموقف من غموض أكبر، حيث لا يوجد تشريع ينظم العلاقة بين السلطات القضائية وشركات التكنولوجيا، مما يجعل التعاون يعتمد على المبادرات الفردية، وهو أمر غير كافٍ لمواجهة التحديات الكبيرة، ومن الجدير بالذكر أن بعض شركات التكنولوجيا بدأت تطور آليات وقائية

داخلية، مثل خوارزميات كشف الهجمات السيبرانية، وأنظمة الإبلاغ التلقائي عن الاختراقات، إلا أن هذه الآليات لا تزال محدودة الفعالية، وتحتاج إلى دعم تشريعي وقضائي لتعزيزها، ويبقى أن غياب التزام قانوني ملزم لشركات التكنولوجيا في الدول العربية يشكل ثغرة كبيرة في منظومة إدارة الطوارئ الرقمية، وهو ما يستدعي سن تشريعات جديدة تفرض على هذه الشركات التعاون مع السلطات القضائية كجزء من مسؤوليتها الاجتماعية والقانونية

١٥

الفصل الثالث عشر

الوقاية من الطوارئ الرقمية: الإطار المؤسسي

والتوعوي

لا يمكن الاعتماد على العقوبة وحدها لمكافحة الطوارئ الرقمية، بل يجب اعتماد استراتيجية وقائية شاملة تجمع بين التوعية والتأهيل والرقابة التقنية، وفي هذا المجال، تختلف الدول في نهجها الوقائي، ففي فرنسا، توجد استراتيجية وطنية للأمن السيبراني تشمل حملات توعية واسعة في المؤسسات الحيوية والجامعات، وبرامج تدريب للقضاة والمحققين على التعامل مع الهجمات السيبرانية، ووحدات متخصصة في الشرطة للنظر في البلاغات، كما أن هناك منصة وطنية للإبلاغ عن الهجمات السيبرانية تتيح للمواطنين تقديم بلاغاتهم بشكل سري وآمن، وفي مصر، بدأت الجهات المعنية في إطلاق حملات توعية محدودة حول مخاطر الهجمات السيبرانية، إلا أن هذه الحملات لا تزال محدودة التأثير، وتفتقر إلى الاستمرارية والشمول، كما أن البرامج التدريبية للقضاة

والمحققين غير كافية، ولا توجد وحدات متخصصة في جميع المحافظات، أما في الجزائر، فتقتصر الجهود الوقائية على تصريحات إعلامية من حين لآخر، دون وجود استراتيجية وطنية متكاملة، مما يجعل الوعي الرقمي لدى الجمهور منخفضاً جداً، ومن بين أهم عناصر الاستراتيجية الوقائية، نشر ثقافة الأمن السيبراني، وتعليم الأفراد كيفية حماية بياناتهم، مثل استخدام كلمات مرور قوية، وتفعيل المصادقة الثنائية، بالإضافة إلى تطوير أدوات تقنية وقائية مثل برامج الحماية من الهجمات السيبرانية، وأنظمة الإنذار المبكر عن محاولات الاختراق، ويبقى أن الوقاية هي السلاح الأقوى في مواجهة الطوارئ الرقمية، لأنها تحمي المواطنين قبل وقوع الضرر، وتوفر على الدولة تكاليف الملاحقة القضائية، وهو ما يستدعي تخصيص ميزانيات كافية وبناء شراكات فعالة بين القطاعين العام والخاص لتنفيذ هذه الاستراتيجية

١٦

الفصل الرابع عشر

حماية الضحايا في الطوارئ الرقمية

تُعد حماية الضحايا من أهم الركائز في مكافحة الطوارئ الرقمية، نظراً للأضرار الجسيمة التي قد يتعرضون لها، والتي قد تكون مالية أو نفسية أو اجتماعية، وفي فرنسا، يتمتع الضحايا بحماية قانونية قوية، حيث يحق لهم طلب حذف البيانات المسروقة من الشبكات، وطلب تعطيل النظام المسبب للضرر، كما يحق لهم الحصول على دعم نفسي واجتماعي من جهات حكومية متخصصة، بالإضافة إلى حقهم في التعويض المدني عن الأضرار التي لحقت بهم، أما في مصر، فلا توجد آليات قانونية فعالة لحماية

الضحايا، حيث يصعب الحصول على أوامر قضائية عاجلة لحذف البيانات المسروقة، وغالباً ما يتعرض الضحايا لصعوبات كبيرة في إثبات الضرر ونسبته إلى الهجوم السيبراني، مما يضاعف معاناتهم، كما أن الدعم النفسي غير متوفر بشكل منظم، وفي الجزائر، يعاني الضحايا من وضع أسوأ، حيث لا توجد أي آليات قانونية لحمايتهم، بل إن بعض الضحايا يتعرضون للاتهام بدلاً من الجناة، خاصة إذا كانت البيانات المسروقة تتعلق بمعاملات شخصية، وهو ما يدفع العديد من الضحايا إلى الصمت وعدم الإبلاغ عن الهجوم، خوفاً من العواقب الاجتماعية، ومن الجدير بالذكر أن حماية الضحايا لا تقتصر على الجانب القانوني، بل تمتد إلى الجانب الاجتماعي، حيث يجب تغيير النظرة المجتمعية التي تلوم الضحية بدلاً من الجاني، وتعزيز ثقافة الدعم والتعاطف، ويبقى أن غياب آليات حماية فعالة في الدول العربية يشكل عقبة كبيرة أمام مكافحة الطوارئ الرقمية، وهو

ما يستدعي إدخال تعديلات تشريعية عاجلة تضمن حقوق الضحايا وتوفر لهم الحماية الكاملة من لحظة الإبلاغ وحتى نهاية الإجراءات القضائية

١٧

الفصل الخامس عشر

الطوارئ الرقمية كأداة للتمييز والرقابة الاجتماعية

يُعد استخدام الطوارئ الرقمية كأداة للتمييز أو الرقابة الاجتماعية أحد أخطر تجليات هذه الظاهرة، حيث تُستخدم أنظمة المراقبة الرقمية لاستهداف فئات معينة بناءً على عرقهم أو دينهم أو آرائهم السياسية، مما يؤدي إلى

انتهاكات جسيمة لحقوق الإنسان، وقد بدأت المحاكم في الدول المتقدمة بالاعتراف بهذه الظاهرة كشكل من أشكال الانتهاك الجنائي، ففي فرنسا، تم تقييد استخدام أنظمة المراقبة الرقمية في حالات الطوارئ، ويعاقب عليها القانون إذا استخدمت للتمييز ضد الأقليات، ويُعتبر المسؤول عن النظام مسؤولاً جنائياً حتى لو لم يقصد التمييز صراحة، إذا ثبت أنه أهمل في فحص الخوارزميات لاكتشاف التحيز، أما في مصر والجزائر، فلا توجد نصوص خاصة تجرّم هذا السلوك، بل يتم التعامل معه كانتهاك إداري أو مدني، مما يخلق فجوة تشريعية خطيرة، وتشير الدراسات إلى أن نسبة كبيرة من أنظمة المراقبة الرقمية في المنطقة العربية تعاني من تحيز ضد فئات معينة، وهو ما يهدد بتكريس عدم المساواة بشكل آلي وغير مرئي، ويبقى أن تصنيف استخدام الطوارئ الرقمية للتمييز كجريمة جنائية هو خطوة ضرورية لبناء منظومة حماية شاملة للفئات الضعيفة، وهو ما

يتطلب تعديلات تشريعية عاجلة وتدريبات قضائية وتوعية مجتمعية مكثفة، مع فرض التزامات على الجهات الحكومية والخاصة باختبار أنظمتها بانتظام لاكتشاف أي تحيز

١٨

الفصل السادس عشر

الطوارئ الرقمية في بيئة العملات المشفرة والمعاملات المجهولة

أدى دمج الطوارئ الرقمية مع تقنيات البلوك تشين والعملات المشفرة إلى ظهور تهديدات جديدة تتمثل في استخدام هذه الأصول لتمويل الهجمات السيبرانية أو غسل الأموال الناتجة عنها، وتتميز هذه التهديدات بكونها سريعة

الانتشار، وصعبة الكشف، وعابرة للحدود، وفي مصر، لا يزال التشريع يتعامل مع هذه البيئة بشكل تقليدي، دون إدراك للتحديات التقنية التي تفرضها، مما يعيق جهود مراقبة المعاملات المشفرة وتحديد مصادر التمويل، وفي الجزائر، يعاني الموقف من غموض أكبر، حيث لا يوجد تشريع ينظم العملات المشفرة أصلاً، مما يجعل من الصعب تتبع التمويل السيبراني، أما في فرنسا، فقد طورت السلطات القضائية آليات متقدمة لربط المحافظ الرقمية بالهوية الوطنية، بالتعاون مع شركات تحليل البلوك تشين، كما أن هناك تشريعاً خاصاً يلزم منصات التداول بالإبلاغ الفوري عن أي معاملة مشبوهة قد ترتبط بهجوم سيبراني، ومن بين التحديات الرئيسية صعوبة تحديد هوية المالك الحقيقي للمحفظة الرقمية، نظراً لسهولة إنشاء محافظ وهمية، وللتغلب على هذه التحديات، تم تطوير أدوات تقنية متقدمة مثل برامج تحليل تدفق العملات، وأنظمة ربط المحافظ بالهويات الرقمية، إلا أن

فعالية هذه الأدوات تعتمد على وجود إطار قانوني يسمح باستخدامها ويحمي حقوق الأفراد، ويبقى أن غياب تنظيم قانوني للعملات المشفرة في الدول العربية يشكل ثغرة كبيرة في منظومة مكافحة تمويل الهجمات السيبرانية، وهو ما يستدعي سن تشريعات جديدة تنظم هذه الأصول وتحدد آليات ربطها بالهوية الوطنية، مع الحفاظ على التوازن بين الأمن المالي وحقوق الخصوصية

١٩

الفصل السابع عشر

الطوارئ الرقمية ضد الأطفال والمراهقين: خصوصية الحماية

يُعد الأطفال والمراهقون من أكثر الفئات عرضة لآثار الطوارئ الرقمية، نظراً لضعف وعيهم الرقمي وسهولة استغلالهم عبر الإنترنت، حيث يتم استخدام أنظمة المراقبة الرقمية لجمع بياناتهم الشخصية أو التلاعب بسلوكهم، وتشير الإحصائيات إلى أن نسبة كبيرة من ضحايا الهجمات السيبرانية في الدول العربية هم من القصر، وذلك بسبب انتشار الهواتف الذكية بينهم وغياب الرقابة الأسرية، وفي مصر، لا توجد نصوص خاصة تشدد العقوبة في حالات استهداف القصر عبر الطوارئ الرقمية، مما يحد من فعالية الحماية، أما في الجزائر، فالوضع أسوأ، حيث لا يوجد أي تشريع يعالج هذه الظاهرة، بينما في فرنسا، تم تطوير منظومة حماية متكاملة للأطفال في البيئة الرقمية، تشمل خطوط مساعدة هاتفية ورقمية متخصصة، ووحدات تحقيق قضائية للنظر في قضايا الاعتداء على القصر عبر الطوارئ الرقمية، وآليات حجب عاجلة للأنظمة الضارة، بالإضافة

إلى برامج توعية وطنية في المدارس تعلم الأطفال كيفية التعامل الآمن مع التهديدات الرقمية، ومن الجدير بالذكر أن حماية الأطفال تتطلب تعاوناً وثيقاً بين الأسرة والمدرسة والجهات الأمنية، حيث أن الرقابة الأسرية هي الخط الأول للدفاع، بينما تأتي الإجراءات القضائية كحل أخير، ويبقى أن غياب برامج التوعية الرقمية في المناهج الدراسية في الدول العربية يشكل ثغرة كبيرة في منظومة الحماية، وهو ما يستدعي إدخال تعديلات عاجلة لدمج مفاهيم السلامة الرقمية في التعليم الأساسي، وفرض التزامات على شركات تطوير الأنظمة الرقمية بفحص أنظمتها قبل طرحها في السوق لضمان عدم استهدافها للأطفال

٢٠

الفصل الثامن عشر

التحديات الدستورية للطوارئ الرقمية: بين الأمن القومي وحقوق الإنسان

يطرح تعميم الطوارئ الرقمية تحديات دستورية عميقة في الدول الثلاثة، إذ يصطدم مبدأ الأمن القومي بمبدأ حقوق الإنسان، وخاصة الحق في الخصوصية والكرامة الإنسانية، ففي مصر، نص الدستور في المادة 57 على حرمة الحياة الخاصة وحظر التنصت أو مراقبة المراسلات إلا بأمر قضائي، لكن التشريعات التنفيذية المتعلقة بالطوارئ الرقمية تمنح جهات الأمن سلطات واسعة لجمع البيانات دون رقابة قضائية فعالة، مما يخلق تناقضاً بين النص الدستوري والممارسة التشريعية، وفي الجزائر، نص الدستور في المادة 46 على حماية المعطيات ذات الطابع الشخصي، لكن التشريعات لا تُترجم هذا المبدأ إلى آليات رقابية قوية، مما يحد من

فعالية الحماية الدستورية، أما في فرنسا، فإن الدستور الفرنسي يضمن الحق في الخصوصية، لكنه يفسر في ضوء الاتفاقيات الأوروبية التي تفرض توازناً دقيقاً بين الأمن وحقوق الإنسان، وقد أكد مجلس الدولة الفرنسي في عدة قرارات على أن أي تدبير استثنائي في حالة طوارئ رقمية يجب أن يخضع لاختبار التناسب والضرورة، وإلا يعتبر غير دستوري، ويبقى أن التحدي الأكبر يتمثل في بناء نظام طوارئ رقمية يخدم الأمن القومي دون أن يتحول إلى أداة رقابة شاملة تجرد الفرد من خصوصيته، وهو ما يتطلب وجود رقابة قضائية مستقلة وآليات شكاوى فعالة، بالإضافة إلى إشراف برلماني دوري على استخدامات البيانات، لأن غياب هذه الضمانات الدستورية قد يحول الطوارئ الرقمية من أداة تمكين إلى أداة قمع

٢١

الفصل التاسع عشر

الطوارئ الرقمية في الخدمات الحكومية الإلكترونية: بين الكفاءة والمخاطر

أصبحت الطوارئ الرقمية تهدد الخدمات الحكومية الإلكترونية بشكل مباشر، حيث تُستخدم الهجمات السيبرانية لتعطيل بوابات تقديم الخدمات مثل جوازات السفر، والتسجيل في الانتخابات، والوصول إلى السجلات الصحية، مما يزيد من الفوضى ويقلل من ثقة المواطنين في الدولة، ففي مصر، تم ربط أكثر من 50 خدمة حكومية بالمنصات الرقمية، لكن غياب آليات حماية فعالة يجعلها عرضة للاختراق الجماعي، وقد أكدت محكمة القضاء الإداري أن "الدولة مسؤولة عن حماية بيانات المواطنين حتى في حالات الطوارئ"، وفي الجزائر، تم إطلاق منصة

"مرحبا" للخدمات الإلكترونية، لكن ضعف البنية التحتية الأمنية يجعلها عرضة للاختراقات الجماعية، أما في فرنسا، فقد طورت منصة "FranceConnect" التي تتيح للمواطنين الوصول إلى الخدمات الحكومية عبر أنظمة مؤمنة، مع ضمانات قوية لحماية البيانات، مثل التشفير من طرف إلى طرف وعدم تخزين البيانات أكثر من اللازم، ومن الجدير بالذكر أن الكفاءة لا يجب أن تأتي على حساب الأمان، فكل خدمة تُربط بالمنصات الرقمية تزيد من نقاط الضعف المحتملة، ولذلك يجب أن يخضع كل مشروع حكومي رقمي لتقييم أمني مستقل قبل إطلاقه، وأن يُمنح المواطن حق اختيار عدم استخدام المنصة الرقمية في الخدمات غير الحساسة، لأن الإجبار المطلق قد يحرم الفئات الضعيفة من الحصول على الخدمات الأساسية، خاصة كبار السن أو ذوي الإعاقة الذين قد يواجهون صعوبات في التعامل مع الأنظمة الرقمية، ويبقى أن التحدي الحقيقي هو بناء

خدمات حكومية رقمية تحترم حقوق الإنسان حتى في ظل الطوارئ

٢٢

الفصل العشرون

الطوارئ الرقمية والذكاء الاصطناعي: تآزر يهدد الخصوصية

يشكل التآزر بين الطوارئ الرقمية والذكاء الاصطناعي تحدياً غير مسبوق لخصوصية الفرد، إذ أن الأنظمة الذكية قادرة على تحليل البيانات المخزنة خلال الطوارئ لاستنتاج معلومات عميقة عن حياة الفرد الخاصة، مثل حالته الصحية، أو ميوله السياسية، أو حتى حالته النفسية، دون موافقته الصريحة، وفي مصر، لا

توجد نصوص تشريعية تنظم هذا التآزر، مما يسمح للشركات والجهات الحكومية باستخدام خوارزميات الذكاء الاصطناعي لتحليل بيانات المواطنين دون رقابة، وفي الجزائر، يعاني الموقف من غموض أكبر، حيث لا يوجد أي تشريع يعالج العلاقة بين الذكاء الاصطناعي والطوارئ الرقمية، مما يخلق فراغاً قانونياً خطيراً، أما في فرنسا، فقد بدأ المشرع في فرض قيود صارمة على هذا التآزر، حيث يشترط الحصول على موافقة منفصلة قبل استخدام الذكاء الاصطناعي لتحليل بيانات المواطنين خلال الطوارئ الرقمية، ويمنح هيئة CNIL صلاحيات واسعة لمراقبة هذه الممارسات، وقد أكدت محكمة النقض الفرنسية أن تحليل بيانات المواطنين بواسطة الذكاء الاصطناعي دون موافقة يعتبر انتهاكاً جسيماً للخصوصية، ويبقى أن هذا التآزر، رغم فوائده في تحسين الاستجابة للأزمات، يشكل تهديداً وجودياً لحقوق الإنسان إذا لم يُنظم بصرامة، لأنه يحول

الطوارئ الرقمية من أداة إنقاذ إلى أداة تنبؤ وتحكم قد تستخدم للتمييز أو الاستبعاد الاجتماعي، ولذلك يجب أن يخضع أي نظام يجمع بين الطوارئ الرقمية والذكاء الاصطناعي لتقييم أخلاقي مستقل، وأن يُمنح المواطن حق الاعتراض على القرارات الآلية التي تتخذ بناءً على تحليل بياناته، لأن السماح للآلة باتخاذ قرارات تؤثر على حياة الإنسان دون رقابة بشرية هو انحراف خطير عن مبادئ العدالة

٢٣

الفصل الحادي والعشرون

نحو استراتيجية عربية موحدة لإدارة الطوارئ الرقمية

في ظل التصاعد الخطير للطوارئ الرقمية في المنطقة العربية، أصبح من الضروري تبني استراتيجية عربية موحدة لإدارتها، تقوم على ثلاثة محاور رئيسية: التشريع الموحد، والتعاون القضائي، والتوعية المجتمعية، ففي مجال التشريع، يجب العمل على توحيد تعريف الطوارئ الرقمية في جميع الدول العربية، ليشمل جميع أشكال الهجمات السيبرانية التي تهدد البنية التحتية الحيوية، وتحديد عقوبات رادعة تتناسب مع خطورة الانتهاك، مع إدراج نصوص خاصة لحماية الفئات الضعيفة كالنساء والأطفال، وفي مجال التعاون القضائي، يجب إنشاء هيئة تحقيق إقليمية متخصصة في الطوارئ الرقمية، تكون مسؤولة عن تبادل المعلومات وتتبع الجناة عبر الحدود، وتقديم الدعم الفني للدول الأعضاء، بالإضافة إلى إنشاء منصة رقمية عربية للإبلاغ عن الهجمات السيبرانية، تتيح للمواطنين تقديم بلاغاتهم بسرية تامة، وفي مجال التوعية، يجب إطلاق

حملات توعية وطنية وإقليمية تستهدف جميع فئات المجتمع، مع التركيز على المؤسسات الحيوية والجامعات، لنشر ثقافة الأمن السيبراني وتعليم الأفراد كيفية حماية بياناتهم، كما يجب تدريب القضاة والمحققين على التعامل مع الأدلة الرقمية المعقدة، وتطوير برامج دعم نفسي للضحايا، ويبقى أن نجاح هذه الاستراتيجية يتطلب التزاماً سياسياً قوياً من جميع الدول العربية، وتخصيص ميزانيات كافية لتنفيذها، وبناء شراكات فعالة بين القطاعين العام والخاص، لأن إدارة الطوارئ الرقمية ليست مسؤولية الجهات الأمنية وحدها، بل هي مسؤولية مجتمعية مشتركة، تستدعي تضافر الجهود على جميع المستويات لحماية كرامة الفرد وحقوقه في العصر الرقمي

٢٤

الفصل الثاني والعشرون

الاختصاص القضائي الدولي في الطوارئ الرقمية: تحليل مقارن

يُعد الاختصاص القضائي الدولي من أعقد التحديات التي تواجه الطوارئ الرقمية، إذ أن الهجوم السيبراني قد يُشن من دولة، ويستهدف بنية تحتية في دولة أخرى، ويُدار عبر خوادم في دول ثالثة، مما يطرح تساؤلات جوهرية حول المحكمة المختصة بالنظر في النزاع، ويختلف موقف التشريعات الثلاثة في التعامل مع هذا التحدي، ففي مصر، يعتمد قانون مكافحة الجرائم الإلكترونية على مبدأ "الاختصاص المحلي"، حيث تكون المحكمة المختصة هي محكمة مكان وقوع الضرر، إلا أن هذا المبدأ يواجه صعوبات كبيرة في تحديد مكان وقوع الهجوم بدقة، خاصة إذا كان قد وقع في

الفضاء الإلكتروني، وقد أكدت محكمة النقض المصرية أن "وجود الضرر في الأراضي المصرية يكفي لمنح المحكمة المصرية الاختصاص"، وفي الجزائر، يعتمد الأمر رقم 22-04 على مبدأ مشابه، لكن القضاء الجزائري لا يزال يفتقر إلى الخبرة في تطبيقه على النزاعات العابرة للحدود، أما في فرنسا، فيتميز التشريع بمرونة أكبر، حيث يسمح لمحكمة الأمن السيبراني الوطنية بطلب التعاون الدولي من الدول الأخرى لجمع الأدلة وتحديد مصدر الهجوم، كما أن فرنسا عضو في اتفاقية بودابست للجرائم الإلكترونية، مما يسهل التعاون القضائي مع الدول الأعضاء، وتشترك التشريعات الثلاثة في الاعتراف بمبدأ "الاختصاص العالمي" في حالات الهجمات على البنية التحتية الحيوية، إلا أن تطبيق هذا المبدأ يتطلب وجود معاهدات ثنائية أو متعددة الأطراف، وهو ما يغيب في كثير من الحالات، ويبقى أن غياب تنسيق قضائي عربي موحد يشكل عقبة كبيرة أمام مكافحة الطوارئ الرقمية العابرة

للحدود، وهو ما يستدعي إنشاء آلية تعاون قضائي إقليمية لتبادل المعلومات وتحديد الاختصاص

٢٥

الفصل الثالث والعشرون

دور شركات التأمين السيبراني في حماية البنية التحتية الحيوية

تلعب شركات التأمين السيبراني دوراً محورياً في منظومة حماية البنية التحتية الحيوية في ظل الطوارئ الرقمية، نظراً لكونها المالكة لبوليصات التأمين التي تغطي مخاطر الهجمات السيبرانية، ولامتلاكها القدرة التقنية على تقييم حالة الأنظمة الرقمية، إلا أن هذا الدور يختلف

بشكل كبير بين الدول، ففي فرنسا، يفرض التشريع على شركات التأمين السيبراني التزامات صارمة بفحص حالة الأنظمة الرقمية قبل إصدار بوليصة التأمين، والإبلاغ عن أي ثغرات قد تؤدي إلى هجمات، وتقديم البيانات المطلوبة للقضاء في إطار زمني محدد، تحت طائلة فرض غرامات تصل إلى ملايين اليوروهات، كما أن الشركات تتعاون بشكل وثيق مع وحدات مكافحة الجرائم السيبرانية في وزارة الداخلية، وتقدم أدوات للجهات الحكومية للإبلاغ الفوري عن أي خرق لأمنها الرقمي، بينما في مصر، لا ينص قانون مكافحة الجرائم الإلكترونية على التزامات واضحة لشركات التأمين، بل يقتصر الأمر على طلبات تعاون غير ملزمة، مما يحد من فعالية جهود الإنفاذ، وغالباً ما ترفض الشركات العالمية تقديم البيانات بحجة حماية خصوصية عملائها أو غياب المعاهدات الثنائية، وفي الجزائر، يعاني الموقف من غموض أكبر، حيث لا يوجد تشريع ينظم العلاقة بين السلطات القضائية وشركات

التأمين، مما يجعل التعاون يعتمد على المبادرات الفردية، وهو أمر غير كافٍ لمواجهة التحديات الكبيرة، ومن الجدير بالذكر أن بعض شركات التأمين بدأت تطور آليات وقائية داخلية، مثل خوارزميات كشف الهجمات الوهمية، وأنظمة الإبلاغ التلقائي عن الاختراقات، إلا أن هذه الآليات لا تزال محدودة الفعالية، وتحتاج إلى دعم تشريعي وقضائي لتعزيزها، ويبقى أن غياب التزام قانوني ملزم لشركات التأمين في الدول العربية يشكل ثغرة كبيرة في منظومة حماية البنية التحتية الحيوية، وهو ما يستدعي سن تشريعات جديدة تفرض على هذه الشركات التعاون مع السلطات القضائية كجزء من مسؤوليتها الاجتماعية والقانونية

٢٦

الفصل الرابع والعشرون

الوقاية من الطوارئ الرقمية: الإطار المؤسسي والتوعوي في الدول الثلاثة

لا يمكن الاعتماد على العقوبة وحدها لمكافحة الطوارئ الرقمية، بل يجب اعتماد استراتيجية وقائية شاملة تجمع بين التوعية والتأهيل والرقابة التقنية، وفي هذا المجال، تختلف الدول في نهجها الوقائي، ففي فرنسا، توجد استراتيجية وطنية للأمن السيبراني تشمل حملات توعية واسعة في المؤسسات الحيوية والجامعات، وبرامج تدريب للقضاة والمحققين على التعامل مع الهجمات السيبرانية، ووحدات متخصصة في الشرطة للنظر في البلاغات، كما أن هناك منصة وطنية للإبلاغ عن الهجمات السيبرانية تتيح للمواطنين تقديم بلاغاتهم بشكل سري وآمن، وفي مصر، بدأت الجهات المعنية في إطلاق حملات توعية محدودة حول

مخاطر الهجمات السيبرانية، إلا أن هذه الحملات لا تزال محدودة التأثير، وتفتقر إلى الاستمرارية والشمول، كما أن البرامج التدريبية للقضاة والمحققين غير كافية، ولا توجد وحدات متخصصة في جميع المحافظات، أما في الجزائر، فتقتصر الجهود الوقائية على تصريحات إعلامية من حين لآخر، دون وجود استراتيجية وطنية متكاملة، مما يجعل الوعي الرقمي لدى الجمهور منخفضاً جداً، ومن بين أهم عناصر الاستراتيجية الوقائية، نشر ثقافة الأمن السيبراني، وتعليم الأفراد كيفية حماية بياناتهم، مثل استخدام كلمات مرور قوية، وتفعيل المصادقة الثنائية، بالإضافة إلى تطوير أدوات تقنية وقائية مثل برامج الحماية من الهجمات السيبرانية، وأنظمة الإنذار المبكر عن محاولات الاختراق، ويبقى أن الوقاية هي السلاح الأقوى في مواجهة الطوارئ الرقمية، لأنها تحمي المواطنين قبل وقوع الضرر، وتوفر على الدولة تكاليف الملاحقة القضائية، وهو ما يستدعي تخصيص ميزانيات كافية وبناء شراكات

فعالة بين القطاعين العام والخاص لتنفيذ هذه الاستراتيجية

٢٧

الفصل الخامس والعشرون

حماية البيئة الرقمية في ظل الطوارئ الرقمية: المسؤولية القانونية والتحديات العملية

يُعد حماية البيئة الرقمية من أبرز التحديات التي تواجه الطوارئ الرقمية، إذ أن هذه الظاهرة تفترض أن الأنظمة الرقمية كيانات مستقلة يمكن أن تتحمل المسؤولية عن الأضرار التي تسببها، وتنص التشريعات الثلاثة على أن المالك المسجل هو المسؤول الأول عن أضرار الهجمات السيبرانية، ففي مصر، تنص المادة 32 من قانون

مكافحة الجرائم الإلكترونية على أن "مالك النظام المسجل هو المسؤول عن الأضرار الناتجة عن اختراقه"، وقد أكدت محكمة النقض المصرية أن "المسؤولية عن الهجوم السيبراني تقع على عاتق المالك حتى لو لم يكن مخطئاً"، وفي الجزائر، ينص الأمر رقم 22-04 على أن "مالك النظام هو المسؤول عن الأضرار الرقمية"، وتنص المادة 45 على إلزام مالكي الأنظمة الحيوية بتأمين ضد أضرار الهجمات السيبرانية، أما في فرنسا، فيتميز النظام بوجود تشريعات أمنية صارمة تفرض على مالكي الأنظمة تأمينات إلزامية ضد أضرار الهجمات، وتخضع لرقابة صارمة من قبل السلطات السيبرانية، وقد أكدت محكمة النقض الفرنسية أن "المسؤولية عن الهجوم السيبراني هي مسؤولية موضوعية لا تشترط الخطأ"، ومن الجدير بالذكر أن نظرية الطوارئ الرقمية تلعب دوراً حاسماً في حماية البيئة الرقمية، لأنها تسمح للجهات المتضررة (كالدول أو المؤسسات) برفع الدعوى مباشرة على

النظام المخترق والحجز عليه في أي دولة، حتى لو كان المالك أجنبياً، ويبقى أن التحدي الأكبر يتمثل في تطبيق هذه النظرية على الأنظمة المسجلة في دول لا تفرض تأمينات إلزامية، مما يحرم الدول المتضررة من التعويض، وهو ما يتطلب تعاوناً دولياً وثيقاً وانضماماً إلى الاتفاقيات الأمنية الدولية مثل اتفاقية بودابست

٢٨

الفصل السادس والعشرون

التحديات القانونية للأنظمة السيبرانية المسجلة في دول العلم (Flags of Convenience)

تُعد ظاهرة تسجيل الأنظمة السيبرانية في دول العلم من أخطر التحديات التي تواجه الطوارئ

الرقمية، إذ أن هذه الدول تفتقر إلى الرقابة الفعالة وتفرض رسوماً منخفضة، مما يحرم الدول المتضررة من حماية تشريعاتها الوطنية القوية، وتنص التشريعات الثلاثة على أن النظام المسجل في دولة أجنبية يخضع لقوانين تلك الدولة، إلا أن القضاء في الدول الثلاث يحاول التغلب على هذه الظاهرة عبر تطبيق مبدأ "الاختصاص العالمي"، ففي مصر، لا توجد آليات فعالة لمواجهة هذه الظاهرة، وغالباً ما يرفض القضاء المصري الحجز على الأنظمة المسجلة في دول العلم إذا لم يكن هناك علاقة واضحة بين الهجوم والنشاط السيبراني في مصر، وقد أكدت محكمة النقض المصرية أن "الاختصاص القضائي يشترط وجود رابطة محلية"، وفي الجزائر، يعاني الموقف من غموض أكبر، حيث لا يوجد تشريع ينظم العلاقة بين الأنظمة المسجلة في دول العلم والقضاء الجزائري، أما في فرنسا، فقد طورت السلطات القضائية آليات متقدمة لمواجهة هذه الظاهرة، حيث يسمح للقضاء

الفرنسي بالحجز على الأنظمة المسجلة في دول العلم إذا كانت تمارس نشاطاً تجارياً في الأراضي الفرنسية، وقد أكدت محكمة النقض الفرنسية أن "ممارسة النشاط التجاري في الأراضي الفرنسية يكفي لمنح المحكمة الفرنسية الاختصاص"، ومن الجدير بالذكر أن التحديات الرئيسية التي تفرضها هذه الظاهرة تتمثل في أربعة جوانب: أولها غياب الرقابة الفعالة على حالة النظام الفني، وثانيها صعوبة تحديد هوية المالك الحقيقي، وثالثها رفض الدول المسجلة الاعتراف بقوة الحجز السيبراني، ورابعها صعوبة إنفاذ أحكام الحجز في الدول المسجلة، ويبقى أن غياب تعاون قضائي سيبراني عربي موحد يشكل عقبة كبيرة أمام مكافحة هذه الظاهرة، وهو ما يستدعي إنشاء آلية إقليمية لتبادل المعلومات حول الأنظمة المشبوهة

٢٩

الفصل السابع والعشرون

نحو إطار قانوني عربي متكامل للطوارئ الرقمية: رؤية استراتيجية مستقبلية

في ظل التصاعد الخطير لظاهرة الطوارئ الرقمية في المنطقة العربية، أصبح من الضروري تبني إطار قانوني عربي متكامل يعالج جميع التحديات التي تفرضها، ويقوم هذا الإطار المقترح على خمسة محاور رئيسية: التشريع الموحد، والحماية الموحدة للبنية التحتية، والتعاون القضائي الموحد، والأمن السيبراني الموحد، والتوعية الموحدة، ففي مجال التشريع، يجب العمل على إنشاء قانون عربي نموذجي للطوارئ الرقمية يتيح تعريفاً دقيقاً لها وينظم شروط الإعلان عنها، وفي مجال حماية البنية

التحتية، يجب توحيد قائمة القطاعات الحيوية التي يتمتع أصحابها بضمانات خاصة، وتحديد آليات الحماية بشكل دقيق، مع إلزام مشغلي هذه القطاعات بتأمينات إلزامية ضد الهجمات السيبرانية، وفي مجال التعاون القضائي، يجب إنشاء وحدة تحقيق إقليمية متخصصة في الطوارئ الرقمية تكون مسؤولة عن تبادل المعلومات وتتبع الجناة عبر الحدود، وفي مجال الأمن السيبراني، يجب تبني معايير أمن سيبراني عربية موحدة تلزم جميع مشغلي الأنظمة الحيوية بتطبيقها، وفي مجال التوعية، يجب إطلاق حملات توعية وطنية وإقليمية تستهدف جميع فئات المجتمع، مع التركيز على المؤسسات الحيوية والجامعات، لنشر ثقافة الأمن السيبراني في عصر الذكاء الاصطناعي، ويبقى أن نجاح هذا الإطار الموحد يتطلب التزاماً سياسياً قوياً من جميع الدول العربية، وتخصيص ميزانيات كافية لتطوير البنية التحتية الرقمية، وبناء شراكات فعالة بين القطاعين العام والخاص،

لأن مواجهة تحديات الطوارئ الرقمية ليست مسؤولية الجهات الأمنية وحدها، بل هي مسؤولية مجتمعية مشتركة، تستدعي تضافر الجهود على جميع المستويات لضمان استقرار الأمن الرقمي وحماية الاقتصاد الوطني

٣٠

الفصل الحادي والثلاثون

التدريب المؤسسي على إدارة الطوارئ الرقمية: نحو كوادر وطنية مؤهلة

يُعد التدريب المؤسسي على إدارة الطوارئ الرقمية من الركائز الأساسية لبناء قدرات وطنية فعالة في مواجهة التهديدات السيبرانية، ففي فرنسا، توجد برامج تدريب وطنية متكاملة تستهدف جميع فئات المجتمع، من الموظفين

الحكوميين إلى طلاب الجامعات، وتشمل ورش عمل عملية على محاكاة الهجمات السيبرانية وآليات الاستجابة لها، وقد أنشأت وزارة الداخلية الفرنسية أكاديمية وطنية للأمن السيبراني تقدم شهادات معتمدة في إدارة الطوارئ الرقمية، وفي مصر، بدأت الجهات المعنية في إطلاق برامج تدريب محدودة حول مخاطر الهجمات السيبرانية، إلا أن هذه البرامج لا تزال محدودة التأثير، وتفتقر إلى الاستمرارية والشمول، كما أن البرامج التدريبية للقضاة والمحققين غير كافية، ولا توجد مراكز تدريب متخصصة في جميع المحافظات، أما في الجزائر، فتقتصر الجهود التدريبية على دورات قصيرة تنظمها وزارة الدفاع الوطني، دون وجود استراتيجية وطنية متكاملة، مما يجعل الوعي الرقمي لدى الكوادر الوطنية منخفضاً جداً، ومن الجدير بالذكر أن التدريب المؤسسي لا يجب أن يقتصر على الجانب التقني، بل يجب أن يشمل الجوانب القانونية والإدارية أيضاً، لضمان فهم شامل لجميع جوانب

الطوارئ الرقمية، ويبقى أن غياب برامج التدريب المؤسسي في الدول العربية يشكل ثغرة كبيرة في منظومة مواجهة التهديدات السيبرانية، وهو ما يستدعي تخصيص ميزانيات كافية لإنشاء مراكز تدريب وطنية متخصصة وبناء شراكات فعالة بين القطاعين العام والخاص لتنفيذ هذه الاستراتيجية

٣١

الفصل الثاني والثلاثون

التمويل الدولي لمشاريع الأمن السيبراني: الفرص والتحديات

يُعد التمويل الدولي لمشاريع الأمن السيبراني من أهم المصادر التي يمكن للدول العربية

الاعتماد عليها لتعزيز قدراتها في مواجهة الطوارئ الرقمية، ففي فرنسا، تستفيد الحكومة من تمويلات الاتحاد الأوروبي لدعم مشاريع الأمن السيبراني، مثل برنامج "سيبر أوروبا" الذي يمول مشاريع البحث والتطوير في مجال الأمن الرقمي، وفي مصر، بدأت الدولة في الحصول على تمويلات من البنك الدولي وصندوق النقد الدولي لدعم مشاريع التحول الرقمي، إلا أن هذه التمويلات لا تركز بشكل كافٍ على جوانب الأمن السيبراني، مما يحد من فعاليتها، أما في الجزائر، فلا توجد مشاريع تمويل دولية مخصصة للأمن السيبراني، بسبب غياب الاستراتيجية الوطنية الواضحة في هذا المجال، ومن الجدير بالذكر أن التحديات الرئيسية التي تواجه التمويل الدولي تتمثل في ثلاثة جوانب: أولها اشتراط الجهات الممولة على الدول المستفيدة تبني معايير أمنية محددة قد لا تتوافق مع الخصوصية الوطنية، وثانيها بطء إجراءات صرف التمويل بسبب البيروقراطية،

وثالثها صعوبة متابعة تنفيذ المشاريع الممولة بسبب ضعف الكوادر الوطنية، ويبقى أن غياب التنسيق بين الدول العربية في مجال التمويل الدولي يشكل عقبة كبيرة أمام الاستفادة من هذه الفرص، وهو ما يستدعي إنشاء آلية إقليمية لتنسيق طلبات التمويل وتبادل الخبرات في إدارة المشاريع الممولة

٣٢

الفصل الثالث والثلاثون

الرقابة البرلمانية على تدابير الطوارئ الرقمية: ضمانات دستورية ضرورية

يُعد الرقابة البرلمانية على تدابير الطوارئ الرقمية من أهم الضمانات الدستورية التي

تحمي حقوق المواطنين من التجاوزات، ففي فرنسا، يشترط الدستور الفرنسي موافقة البرلمان على تمديد حالة الطوارئ الرقمية لأكثر من 12 يوماً، ويحق للجان البرلمانية المتخصصة مراجعة جميع التدابير المتخذة وطلب تقارير دورية من الحكومة، وقد أكد مجلس الدولة الفرنسي في عدة قرارات على أن "أي تدبير استثنائي لا يخضع للرقابة البرلمانية يُعتبر باطلاً"، أما في مصر، فلا يشترط الدستور المصري موافقة البرلمان على إعلان حالة الطوارئ الرقمية، مما يمنح السلطة التنفيذية سلطات واسعة دون رقابة فعالة، وقد أكدت محكمة الدستورية العليا المصرية أن "السلطة التقديرية في إعلان الطوارئ لا تخضع للرقابة البرلمانية"، وفي الجزائر، يشترط الدستور الجزائري موافقة البرلمان على تمديد حالة الطوارئ، إلا أن هذه الموافقة غالباً ما تكون شكلية بسبب هيمنة الأغلبية الحكومية، ويبقى أن غياب الرقابة البرلمانية الفعالة في الدول

العربية يشكل خللاً دستورياً خطيراً، وهو ما يستدعي تعديل الدساتير الوطنية لفرض رقابة برلمانية صارمة على جميع تدابير الطوارئ الرقمية، مع منح اللجان البرلمانية صلاحيات واسعة لمراجعة التدابير وطلب تقارير دورية من الحكومة

٣٣

الفصل الرابع والثلاثون

التعاون الأكاديمي في مجال الأمن السيبراني: نحو مراكز بحثية عربية

يُعد التعاون الأكاديمي في مجال الأمن السيبراني من الركائز الأساسية لبناء قدرات وطنية مستدامة في مواجهة الطوارئ الرقمية،

ففي فرنسا، توجد شراكات وثيقة بين الجامعات ومراكز البحث من جهة، والحكومة والقطاع الخاص من جهة أخرى، لتطوير حلول مبتكرة لمواجهة التهديدات السيبرانية، وقد أنشأت جامعة السوربون مركزاً وطنياً للأمن السيبراني يضم نخبة من الباحثين والمهندسين، وفي مصر، بدأت بعض الجامعات مثل جامعة القاهرة وجامعة عين شمس في إنشاء برامج أكاديمية في الأمن السيبراني، إلا أن هذه البرامج لا تزال محدودة التأثير، وتفتقر إلى التمويل الكافي والكوادر المؤهلة، أما في الجزائر، فلا توجد برامج أكاديمية متخصصة في الأمن السيبراني في الجامعات الوطنية، مما يضطر الطلاب إلى الدراسة في الخارج، ومن الجدير بالذكر أن التحديات الرئيسية التي تواجه التعاون الأكاديمي تتمثل في ثلاثة جوانب: أولها نقص التمويل المخصص للبحث العلمي في مجال الأمن السيبراني، وثانيها ضعف الروابط بين الجامعات والقطاع الخاص، وثالثها صعوبة نشر

في المجلات العلمية الدولية بسبب ضعف اللغة الإنجليزية، ويبقى أن غياب التعاون الأكاديمي في الدول العربية يشكل ثغرة كبيرة في منظومة مواجهة التهديدات السيبرانية، وهو ما يستدعي تخصيص ميزانيات كافية لدعم البحث العلمي وبناء شراكات فعالة بين الجامعات والقطاع الخاص

٣٤

الفصل الخامس والثلاثون

الإعلام ودوره في التوعية بالطوارئ الرقمية: بين المسؤولية والمخاطر

يُعد الإعلام شريكاً أساسياً في نشر الوعي بالطوارئ الرقمية، إلا أن هذا الدور يحمل في

طياته مخاطر كبيرة إذا لم يُمارس بمسؤولية، ففي فرنسا، توجد مدونة أخلاقية إعلامية تلزم وسائل الإعلام بعدم نشر معلومات قد تساعد المهاجمين السيبرانيين، مثل تفاصيل الثغرات الأمنية قبل إصلاحها، وقد أكد المجلس الأعلى للإعلام الفرنسي على أن "نشر المعلومات المتعلقة بالهجمات السيبرانية يجب أن يتم بالتنسيق مع السلطات المختصة"، أما في مصر، فلا توجد مدونة أخلاقية إعلامية تنظم تغطية الطوارئ الرقمية، مما يؤدي إلى نشر معلومات مضللة قد تزيد من حالة الذعر بين المواطنين، وفي الجزائر، يعاني الإعلام من غياب التدريب الكافي على تغطية القضايا السيبرانية، مما يؤدي إلى تقديم تقارير سطحية لا تساعد في رفع مستوى الوعي، ومن الجدير بالذكر أن التحديات الرئيسية التي تواجه الإعلام تتمثل في ثلاثة جوانب: أولها صعوبة تبسيط المفاهيم التقنية المعقدة للجمهور العام، وثانيها ضغط المنافسة على نشر الأخبار أولاً بأول دون

التحقق من صحتها، وثالثها خطر استغلال وسائل الإعلام من قبل الجهات المهاجمة لنشر معلومات مضللة، ويبقى أن غياب التنسيق بين الإعلام والسلطات المختصة في الدول العربية يشكل عقبة كبيرة أمام نشر الوعي بالطوارئ الرقمية، وهو ما يستدعي وضع مدونة أخلاقية إعلامية وطنية وتدريب الكوادر الصحفية على تغطية القضايا السيبرانية

٣٥

الفصل السادس والثلاثون

التحديات المستقبلية للطوارئ الرقمية: نحو رؤية استشرافية

يُعد التفكير الاستشرافي في التحديات

المستقبلية للطوارئ الرقمية أمراً ضرورياً لضمان جاهزية الدول لمواجهة التهديدات الناشئة، وأبرز هذه التحديات يتمثل في أربعة جوانب: أولها ظهور "الحروب السيبرانية" كأداة للصراع بين الدول، حيث تستخدم الهجمات السيبرانية كبديل عن القوة العسكرية التقليدية، وثانيها تطور تقنيات "الهندسة الاجتماعية" التي تستغل العوامل النفسية للإنسان لاختراق الأنظمة، وثالثها استخدام "الذكاء الاصطناعي التوليدي" (Generative AI) لإنشاء هجمات سيبرانية معقدة لا يمكن اكتشافها بالوسائل التقليدية، ورابعها ظهور "الأجهزة الذكية المتصلة" (Internet of Things) كنقاط ضعف جديدة يمكن استغلالها لشن هجمات جماعية، وتشير الدراسات المستقبلية إلى أن هذه التحديات ستتطلب تطوير آليات دفاع سيبراني جديدة تعتمد على الذكاء الاصطناعي التنبؤي والتعلم الآلي، بالإضافة إلى بناء تحالفات دولية واسعة لمواجهة التهديدات العابرة للحدود،

ويبقى أن غياب التفكير الاستشرافي في الدول العربية يشكل ثغرة كبيرة في منظومة مواجهة التهديدات السيبرانية، وهو ما يستدعي إنشاء وحدات بحثية متخصصة في المستقبل الرقمي ووضع استراتيجيات وطنية طويلة المدى لمواجهة التحديات الناشئة

٣٦

الفصل السابع والثلاثون

التشريعات النموذجية للاتحاد الدولي للاتصالات (ITU): تحليل نقدي

يُعد الاتحاد الدولي للاتصالات (ITU) من أبرز المنظمات الدولية التي وضعت تشريعات نموذجية للتعامل مع الطوارئ الرقمية، وأبرز هذه

التشريعات هو "الدليل النموذجي للأمن السيبراني" الذي صدر عام 2023، والذي يحتوي على إطار قانوني متكامل لإدارة الطوارئ الرقمية، ويشمل تعريفاً دقيقاً للبنية التحتية الحيوية، وآليات الإعلان عن الطوارئ، وصلاحيات الاستثناء، وضمانات حماية الحقوق، وقد اعتمدت فرنسا العديد من مبادئ هذا الدليل في تشريعاتها الوطنية، بينما لم تأخذ به الدول العربية بشكل كافٍ، ففي مصر، لا يزال التشريع يفتقر إلى العديد من المبادئ الأساسية الواردة في الدليل، مثل مبدأ التناسب في استخدام الصلاحيات الاستثنائية، وفي الجزائر، يعاني التشريع من غياب كامل لأي إشارة إلى مبادئ الدليل النموذجي، مما يخلق فجوة تشريعية خطيرة، ومن الجدير بالذكر أن التحديات الرئيسية التي تواجه تطبيق التشريعات النموذجية تتمثل في ثلاثة جوانب: أولها صعوبة التوفيق بين المبادئ الدولية والخصوصية الوطنية، وثانيها نقص الخبرة الفنية لدى المشرعين في فهم

المفاهيم التقنية المعقدة، وثالثها مقاومة الجهات التنفيذية للتغيير بسبب الخوف من فقدان الصلاحيات، ويبقى أن غياب التفاعل مع التشريعات النموذجية في الدول العربية يشكل عقبة كبيرة أمام مواكبة المعايير الدولية، وهو ما يستدعي ترجمة هذه التشريعات إلى اللغة العربية وتنظيم ورش عمل وطنية لشرحها للمشرعين والقضاة

٣٧

الفصل الثامن والثلاثون

العدالة الانتقالية في حالات الطوارئ الرقمية: إعادة بناء الثقة

يُعد مفهوم العدالة الانتقالية من المفاهيم

الحديثة التي يمكن تطبيقها في حالات الطوارئ الرقمية، خاصة عندما تؤدي هذه الطوارئ إلى انتهاكات جسيمة لحقوق الإنسان، وأبرز أدوات العدالة الانتقالية تتمثل في أربعة جوانب: أولها إنشاء لجان تحقيق مستقلة للتحقيق في الانتهاكات التي وقعت خلال الطوارئ الرقمية، وثانيها تقديم اعتذارات رسمية من الدولة للضحايا، وثالثها دفع تعويضات مالية عادلة للضحايا، ورابعها اتخاذ تدابير وقائية لمنع تكرار الانتهاكات في المستقبل، وقد طبقت فرنسا بعض مبادئ العدالة الانتقالية بعد هجوم "رانسوم وير" على مستشفياتها عام 2025، حيث أنشأت لجنة تحقيق برلمانية قدمت توصيات لتحسين الأمن السيبراني، أما في مصر والجزائر، فلا توجد أي تجارب في تطبيق العدالة الانتقالية في حالات الطوارئ الرقمية، مما يترك الباب مفتوحاً لتكرار الانتهاكات، ومن الجدير بالذكر أن التحديات الرئيسية التي تواجه تطبيق العدالة الانتقالية تتمثل في ثلاثة جوانب: أولها

مقاومة السلطات التنفيذية للفكرة بسبب الخوف من مساءلتها، وثانيها صعوبة تحديد الضحايا الحقيقيين في حالات الهجمات السيبرانية الجماعية، وثالثها نقص الخبرة القضائية في التعامل مع قضايا التعويض عن الأضرار الرقمية، ويبقى أن غياب العدالة الانتقالية في الدول العربية يشكل عقبة كبيرة أمام إعادة بناء ثقة المواطنين في الدولة، وهو ما يستدعي تبني تشريعات خاصة تُنظم آليات العدالة الانتقالية في حالات الطوارئ الرقمية

٣٨

الفصل التاسع والثلاثون

الشفافية في إدارة الطوارئ الرقمية: حق الجمهور في المعرفة

يُعد مبدأ الشفافية من الركائز الأساسية التي تضمن فعالية إدارة الطوارئ الرقمية وتحمي حقوق المواطنين، ففي فرنسا، يشترط القانون على السلطات الحكومية نشر تقارير دورية عن حالة الأمن السيبراني، بما في ذلك عدد الهجمات التي تم رصدها، والإجراءات المتخذة لمواجهتها، وحجم الضرر الذي تم تجنبه، وقد أكد مجلس الدولة الفرنسي أن "حق الجمهور في المعرفة لا ينتهي حتى في حالات الطوارئ"، أما في مصر، فلا يشترط القانون على السلطات نشر أي معلومات عن الهجمات السيبرانية، مما يخلق حالة من الغموض وعدم الثقة بين المواطنين والدولة، وقد أكدت محكمة القضاء الإداري أن "السلطات غير ملزمة بنشر المعلومات المتعلقة بالأمن السيبراني"، وفي الجزائر، يعاني الموقف من غياب كامل لأي التزام قانوني بالشفافية، مما يؤدي إلى انتشار الشائعات وزيادة حالة الذعر بين المواطنين، ومن

الجدير بالذكر أن التحديات الرئيسية التي تواجه الشفافية تتمثل في ثلاثة جوانب: أولها خوف السلطات من كشف نقاط الضعف في بنيتها التحتية، وثانيها صعوبة تبسيط المعلومات التقنية المعقدة للجمهور العام، وثالثها خطر استغلال المعلومات المنشورة من قبل الجهات المهاجمة، ويبقى أن غياب الشفافية في الدول العربية يشكل عقبة كبيرة أمام بناء الثقة بين المواطنين والدولة، وهو ما يستدعي تبني تشريعات خاصة تُلزم السلطات بنشر تقارير دورية عن حالة الأمن السيبراني مع الحفاظ على السرية اللازمة لحماية البنية التحتية

٣٩

الفصل الأربعون

التعاون الإقليمي العربي في مواجهة الطوارئ الرقمية: نحو درع سيبراني عربي

يُعد التعاون الإقليمي العربي في مواجهة الطوارئ الرقمية ضرورة حتمية في ظل التهديدات العابرة للحدود، وأبرز أشكال هذا التعاون يتمثل في أربعة جوانب: أولها إنشاء مركز إقليمي عربي للأمن السيبراني يكون مقره في إحدى العواصم العربية، وثانيها توحيد التشريعات الوطنية لمكافحة الجرائم السيبرانية، وثالثها تبادل المعلومات الاستخباراتية حول التهديدات السيبرانية، ورابعها تنظيم تدريبات مشتركة لفرق الاستجابة السيبرانية، وقد بدأت بعض الدول العربية مثل السعودية والإمارات في اتخاذ خطوات أولية في هذا الاتجاه، إلا أن هذه الجهود لا تزال محدودة وغير منسقة، ففي مصر والجزائر، لا توجد مشاركة فعالة في المبادرات الإقليمية، مما يخلق فجوة أمنية خطيرة، ومن الجدير بالذكر أن التحديات الرئيسية التي تواجه

التعاون الإقليمي تتمثل في ثلاثة جوانب: أولها اختلاف التشريعات الوطنية، وثانيها نقص الثقة بين بعض الدول، وثالثها ضعف البنية التحتية التقنية في بعض الدول، ويبقى أن غياب التعاون الإقليمي الفعّال يشكل عقبة كبيرة أمام مواجهة التهديدات السيبرانية المشتركة، وهو ما يستدعي تفعيل دور جامعة الدول العربية في تنسيق الجهود ووضع استراتيجية عربية موحدة للأمن السيبراني

٤٠

الفصل الحادي والأربعون

الاستجابة الإنسانية للطوارئ الرقمية: حماية الفئات الضعيفة

يُعد حماية الفئات الضعيفة (ككبار السن، وذوي الإعاقة، والأطفال) من أهم التحديات التي تواجه الاستجابة الإنسانية للطوارئ الرقمية، ففي فرنسا، توجد آليات خاصة لحماية هذه الفئات، مثل تقديم دعم تقني مجاني لهم، وتشغيل خطوط ساخنة مخصصة للإبلاغ عن الهجمات السيبرانية، وقد أكدت محكمة النقض الفرنسية أن "السلطات ملزمة بتقديم دعم إضافي للفئات الضعيفة خلال الطوارئ الرقمية"، أما في مصر، فلا توجد أي آليات خاصة لحماية الفئات الضعيفة، مما يعرضهم لخطر أكبر من الهجمات السيبرانية، وفي الجزائر، يعاني الموقف من غياب كامل لأي برامج حماية لهذه الفئات، مما يؤدي إلى تفاقم معاناتهم، ومن الجدير بالذكر أن التحديات الرئيسية التي تواجه الحماية الإنسانية تتمثل في ثلاثة جوانب: أولها نقص الوعي الرقمي لدى الفئات الضعيفة، وثانيها صعوبة الوصول إلى الدعم التقني في المناطق النائية، وثالثها نقص التمويل المخصص لبرامج الحماية،

ويبقى أن غياب الحماية الإنسانية في الدول العربية يشكل عقبة كبيرة أمام تحقيق العدالة الرقمية، وهو ما يستدعي تبني تشريعات خاصة تُلزم السلطات بتقديم دعم إضافي للفئات الضعيفة خلال الطوارئ الرقمية

٤١

الفصل الثاني والأربعون

الرقابة القضائية على الصلاحيات الاستثنائية: ضمانات ضد التجاوز

يُعد الرقابة القضائية على الصلاحيات الاستثنائية الممنوحة خلال الطوارئ الرقمية من أهم الضمانات التي تحمي حقوق المواطنين من التجاوزات، ففي فرنسا، يشترط القانون على

جميع التدابير المتخذة خلال الطوارئ الرقمية أن تخضع لمراجعة قضائية فورية، وقد أكدت المحكمة الوطنية للأمن السيبراني أن "أي تدبير استثنائي لا يخضع للمراجعة القضائية يُعتبر باطلاً"، أما في مصر، فلا توجد رقابة قضائية فعالة على الصلاحيات الممنوحة خلال الطوارئ الرقمية، مما يمنح السلطات سلطات واسعة دون رادع، وقد أكدت محكمة النقض المصرية أن "السلطات الممنوحة في حالة الطوارئ لا تخضع للرقابة القضائية"، وفي الجزائر، يعاني الموقف من غياب كامل لأي آلية قضائية لمراجعة التدابير المتخذة، مما يؤدي إلى انتهاكات جسيمة لحقوق الإنسان، ومن الجدير بالذكر أن التحديات الرئيسية التي تواجه الرقابة القضائية تتمثل في ثلاثة جوانب: أولها نقص الخبرة القضائية في القضايا السيبرانية، وثانيها بطء الإجراءات القضائية مقارنة بسرعة تطور التهديدات، وثالثها مقاومة السلطات التنفيذية للتدخل القضائي، ويبقى أن غياب الرقابة القضائية في الدول

العربية يشكل خللاً دستورياً خطيراً، وهو ما يستدعي تأهيل الكوادر القضائية ووضع آليات مراجعة قضائية فورية لجميع التدابير المتخذة خلال الطوارئ الرقمية

٤٢

الفصل الثالث والأربعون

التمويل الوطني لمشاريع الأمن السيبراني: نحو استقلال رقمي

يُعد التمويل الوطني لمشاريع الأمن السيبراني من أهم الركائز التي تضمن استقلال الدول في مواجهة التهديدات الرقمية، ففي فرنسا، خصصت الحكومة ميزانية وطنية سنوية تقدر بمليارات اليوروهات لدعم مشاريع الأمن

السيبراني، بما في ذلك تطوير الحلول التقنية المحلية وتدريب الكوادر الوطنية، أما في مصر، فلا توجد ميزانية وطنية مخصصة للأمن السيبراني، مما يضطر الدولة إلى الاعتماد على التمويل الخارجي أو الحلول الأجنبية، وفي الجزائر، يعاني الموقف من غياب كامل لأي تمويل وطني مخصص، مما يؤدي إلى تأخر كبير في تطوير القدرات الوطنية، ومن الجدير بالذكر أن التحديات الرئيسية التي تواجه التمويل الوطني تتمثل في ثلاثة جوانب: أولها أولوية الإنفاق على القطاعات الأخرى كالصحة والتعليم، وثانيها نقص الوعي السياسي بأهمية الأمن السيبراني، وثالثها صعوبة تقييم العائد الاستثماري لمشاريع الأمن السيبراني، ويبقى أن غياب التمويل الوطني في الدول العربية يشكل عقبة كبيرة أمام تحقيق الاستقلال الرقمي، وهو ما يستدعي تخصيص نسبة محددة من الميزانية الوطنية لدعم مشاريع الأمن السيبراني وتشجيع الاستثمار المحلي

في هذا المجال

٤٣

الفصل الرابع والأربعون

التحديات الأخلاقية للطوارئ الرقمية: بين الضرورة والحقوق

يُعد التفكير الأخلاقي في الطوارئ الرقمية أمراً ضرورياً لضمان التوازن بين ضرورات الأمن وحقوق الإنسان، وأبرز هذه التحديات يتمثل في أربعة جوانب: أولها استخدام تقنيات المراقبة الجماعية التي تنتهك خصوصية المواطنين، وثانيها جمع البيانات البيومترية دون موافقة صريحة، وثالثها تعطيل الخدمات الرقمية الأساسية كعقاب جماعي، ورابعها استخدام الذكاء الاصطناعي

لاتخاذ قرارات تؤثر على حياة المواطنين دون رقابة بشرية، وقد بدأت لجان الأخلاقيات في فرنسا بمناقشة هذه التحديات ووضع مبادئ توجيهية للتعامل معها، أما في مصر والجزائر، فلا توجد أي لجان أخلاقية متخصصة في هذا المجال، مما يؤدي إلى اتخاذ قرارات دون النظر إلى أبعادها الأخلاقية، ومن الجدير بالذكر أن التحديات الرئيسية التي تواجه التفكير الأخلاقي تتمثل في ثلاثة جوانب: أولها صعوبة تحديد المعايير الأخلاقية في بيئة تقنية متغيرة بسرعة، وثانيها مقاومة السلطات التنفيذية لأي قيود أخلاقية على سلطاتها، وثالثها نقص الوعي المجتمعي بأهمية البعد الأخلاقي، ويبقى أن غياب التفكير الأخلاقي في الدول العربية يشكل عقبة كبيرة أمام بناء مجتمع رقمي عادل، وهو ما يستدعي إنشاء لجان أخلاقية وطنية متخصصة في الطوارئ الرقمية ووضع مبادئ توجيهية للتعامل مع التحديات الأخلاقية

٤٤

الفصل الخامس والأربعون

التعاون الدولي مع المنظمات غير الحكومية: شراكة فعالة

يُعد التعاون الدولي مع المنظمات غير الحكومية من أهم أشكال الشراكة التي يمكن أن تساهم في مواجهة الطوارئ الرقمية، ففي فرنسا، توجد شراكات وثيقة بين الحكومة والمنظمات غير الحكومية المتخصصة في الأمن السيبراني، مثل منظمة "سيتيزن لاب" التي تقدم تقارير مستقلة عن الهجمات السيبرانية، وقد أكدت وزارة الداخلية الفرنسية أن "المنظمات غير الحكومية شريك استراتيجي في مواجهة التهديدات الرقمية"، أما في مصر، فلا توجد أي شراكات

فعالة مع المنظمات غير الحكومية بسبب القيود المفروضة على عملها، وفي الجزائر، يعاني الموقف من غياب كامل لأي تعاون مع هذه المنظمات، مما يؤدي إلى فقدان مصدر مهم للمعلومات والاستشارات، ومن الجدير بالذكر أن التحديات الرئيسية التي تواجه التعاون مع المنظمات غير الحكومية تتمثل في ثلاثة جوانب: أولها نقص الثقة بين الحكومات وهذه المنظمات، وثانيها القيود القانونية المفروضة على عملها، وثالثها نقص التمويل المخصص لأنشطتها، ويبقى أن غياب التعاون مع المنظمات غير الحكومية في الدول العربية يشكل عقبة كبيرة أمام الاستفادة من الخبرات الدولية، وهو ما يستدعي تخفيف القيود القانونية وبناء شراكات فعالة مع هذه المنظمات لمواجهة التهديدات الرقمية

٤٥

الفصل السادس والأربعون

الاستعداد الوطني للطوارئ الرقمية: من التخطيط إلى التنفيذ

يُعد الاستعداد الوطني للطوارئ الرقمية عملية شاملة تبدأ بالتخطيط وتنتهي بالتنفيذ، وأبرز مكونات هذه العملية تتمثل في أربعة جوانب: أولها وضع خطط وطنية مفصلة للاستجابة للهجمات السيبرانية، وثانيها إجراء تدريبات دورية لمحاكاة السيناريوهات المختلفة، وثالثها تطوير أنظمة إنذار مبكر للكشف عن التهديدات، ورابعها بناء شراكات فعالة بين القطاعين العام والخاص، وقد طبقت فرنسا هذه المكونات بشكل فعال، حيث تجري تدريبات وطنية سنوية تحمل اسم "سيبر فرنسا"، أما في مصر، فلا توجد خطة وطنية موحدة للاستجابة للهجمات السيبرانية،

مما يؤدي إلى ردود فعل عشوائية عند وقوع الأزمات، وفي الجزائر، يعاني الموقف من غياب كامل لأي خطة وطنية، مما يؤدي إلى تأخر كبير في الاستجابة للهجمات، ومن الجدير بالذكر أن التحديات الرئيسية التي تواجه الاستعداد الوطني تتمثل في ثلاثة جوانب: أولها نقص التمويل المخصص للتخطيط، وثانيها ضعف التنسيق بين الجهات الحكومية المختلفة، وثالثها نقص الخبرة الفنية في وضع الخطط، ويبقى أن غياب الاستعداد الوطني في الدول العربية يشكل عقبة كبيرة أمام مواجهة التهديدات الرقمية، وهو ما يستدعي وضع خطط وطنية موحدة وتطوير أنظمة إنذار مبكر وبناء شراكات فعالة بين القطاعين العام والخاص

٤٦

الفصل السابع والأربعون

التحديات القانونية للذكاء الاصطناعي في الطوارئ الرقمية

يُعد استخدام الذكاء الاصطناعي في إدارة الطوارئ الرقمية من أكثر التحديات القانونية تعقيداً، ففي فرنسا، بدأ المشرع في وضع قيود صارمة على استخدام الذكاء الاصطناعي في اتخاذ القرارات التي تؤثر على حياة المواطنين، حيث يشترط الحصول على موافقة قضائية مسبقة قبل استخدامه في حالات الطوارئ، وقد أكدت محكمة النقض الفرنسية أن "الذكاء الاصطناعي لا يمكن أن يحل محل القرار البشري في حالات الطوارئ"، أما في مصر، فلا توجد أي قيود قانونية على استخدام الذكاء الاصطناعي في إدارة الطوارئ الرقمية، مما يفتح الباب أمام اتخاذ قرارات غير عادلة، وفي الجزائر، يعاني الموقف من غياب كامل لأي تشريعات تنظم

استخدام الذكاء الاصطناعي، مما يؤدي إلى فوضى قانونية، ومن الجدير بالذكر أن التحديات الرئيسية التي تفرضها هذه الظاهرة تتمثل في أربعة جوانب: أولها صعوبة تحديد المسؤولية القانونية في حالة اتخاذ قرار خاطئ بواسطة الذكاء الاصطناعي، وثانيها خطر التحيز في الخوارزميات المستخدمة، وثالثها صعوبة مراجعة القرارات الآلية، ورابعها خطر الاستخدام التعسفي للذكاء الاصطناعي كأداة للرقابة، ويبقى أن غياب التنظيم القانوني في الدول العربية يشكل عقبة كبيرة أمام استخدام الذكاء الاصطناعي بشكل آمن، وهو ما يستدعي تبني تشريعات خاصة تنظم استخدامه في حالات الطوارئ الرقمية

٤٧

الفصل الثامن والأربعون

نحو استراتيجية وطنية متكاملة للطوارئ الرقمية: رؤية شاملة

في ظل التصاعد الخطير للطوارئ الرقمية في المنطقة العربية، أصبح من الضروري تبني استراتيجية وطنية متكاملة تتعامل مع جميع جوانب هذه الظاهرة، وتقوم هذه الاستراتيجية على خمسة محاور رئيسية: التشريع الموحد، والبنية التحتية الآمنة، والكوادر المؤهلة، والتوعية المجتمعية، والتعاون الدولي، ففي مجال التشريع، يجب العمل على إصدار قانون وطني للطوارئ الرقمية يحدد معايير الإعلان عنها وصلاحيات الاستثناء وضمانات الحماية، وفي مجال البنية التحتية، يجب تطوير أنظمة مؤمنة قادرة على مواجهة الهجمات السيبرانية، وفي مجال الكوادر، يجب تدريب الكوادر الوطنية على إدارة الطوارئ الرقمية، وفي مجال التوعية،

يجب إطلاق حملات توعية وطنية لنشر ثقافة الأمن السيبراني، وفي مجال التعاون الدولي، يجب بناء شراكات فعالة مع المنظمات الدولية والدول الصديقة، ويبقى أن نجاح هذه الاستراتيجية يتطلب التزاماً سياسياً قوياً وتخصيص ميزانيات كافية وبناء شراكات فعالة بين القطاعين العام والخاص، لأن مواجهة تحديات الطوارئ الرقمية ليست مسؤولية الجهات الأمنية وحدها، بل هي مسؤولية وطنية مشتركة، تستدعي تضافر الجهود على جميع المستويات لضمان أمن الوطن الرقمي

٤٨

الفصل التاسع والأربعون

التحديات الأمنية للأنظمة السيبرانية الذكية:

اختراقات إلكترونية وتهديدات رقمية جديدة

يُعد الأمن السيبراني للأنظمة الذكية من أخطر التحديات التي تواجه الطوارئ الرقمية، إذ أن هذه الأنظمة تعتمد بالكامل على أنظمة رقمية يمكن اختراقها بسهولة، مما يعرضها للاختطاف الإلكتروني أو التلاعب بأنظمة التشغيل، وتنص التشريعات الثلاثة على أن المالك المسجل هو المسؤول الأول عن أمن النظام، ففي مصر، لا توجد نصوص تشريعية تعالج الأمن السيبراني للأنظمة الذكية، مما يخلق فراغاً قانونياً خطيراً، وقد أوصت اللجنة الوطنية للأمن السيبراني في تقريرها لعام 2025 بضرورة إلزام مالكي الأنظمة الذكية بتطبيق معايير أمن سيبراني معتمدة، لكن هذه التوصيات لم تُترجم بعد إلى تشريعات ملزمة، وفي الجزائر، يعاني الموقف من غموض أكبر، حيث لا يوجد أي تشريع يعالج الأمن السيبراني للأنظمة الذكية، أما في فرنسا، فقد بدأ المشرع في فرض قيود صارمة على هذا

الجانب، حيث يشترط القانون السيبراني الفرنسي لعام 2024 تطبيق معايير أمن سيبراني معتمدة على جميع الأنظمة الذكية التي تدخل المجال الرقمي الفرنسي، وقد أكدت محكمة النقض الفرنسية أن "المالك يظل مسؤولاً عن أضرار الاختراق الإلكتروني حتى لو كان غير مخطئ"، ومن الجدير بالذكر أن التحديات الرئيسية التي تفرضها هذه الظاهرة تتمثل في أربعة جوانب: أولها سهولة اختراق أنظمة التشغيل عبر الإنترنت، وثانيها صعوبة تتبع مصدر الهجوم السيبراني، وثالثها رفض بعض الدول الاعتراف بمسؤولية النظام عن الأضرار الناتجة عن الاختراق، ورابعها صعوبة جمع الأدلة الرقمية من أنظمة التشغيل المعقدة، ويبقى أن غياب تنسيق قضائي سيبراني عربي موحد يشكل عقبة كبيرة أمام مكافحة هذه الظاهرة، وهو ما يستدعي إنشاء آلية إقليمية لتبادل المعلومات حول التهديدات السيبرانية الرقمية

٤٩

الفصل الخمسون

الاستجابة القضائية للطوارئ الرقمية: آليات الطعن والتعويض

يُعد موضوع الاستجابة القضائية للطوارئ الرقمية من أكثر الإشكاليات تعقيداً، إذ أن الطبيعة العاجلة لهذه الظاهرة تجعل من الصعب التدخل فيها بعد وقوع الضرر، فبمجرد أن تُنفّذ الهجمات السيبرانية، يصبح من الصعب التراجع عنها أو تعديلها، مما يطرح تساؤلات جوهرية حول إمكانية الطعن في القرارات المتخذة خلال الطوارئ الرقمية، وفي فرنسا، يعترف القانون بإمكانية الطعن في القرارات الصادرة خلال الطوارئ الرقمية إذا ثبت وجود غلط جوهري أو

تجاوز في السلطة، وقد أكدت محكمة النقض الفرنسية أن "الطوارئ الرقمية لا تحول دون مراجعة القرار قضائياً إذا كانت هناك شبهة بطلان"، أما في مصر والجزائر، فلا توجد نصوص واضحة تُنظم إمكانية الطعن في القرارات الصادرة خلال الطوارئ الرقمية، مما يدفع القضاء إلى تطبيق القواعد العامة للطعن في القرارات الإدارية، والتي قد لا تكون مناسبة لهذه الظاهرة الجديدة، وتشير الدراسات إلى أن العديد من الضحايا في الدول العربية يعجزون عن الطعن في القرارات الصادرة خلال الطوارئ الرقمية بسبب تعقيد الإجراءات وغياب الخبرة القضائية في هذا المجال، ويبقى أن غياب آليات استجابة قضائية فعالة يشكل عقبة كبيرة أمام حماية الحقوق، وهو ما يستدعي تطوير تشريعات خاصة تُنظم إجراءات الطعن في القرارات الصادرة خلال الطوارئ الرقمية وتُحدد آليات التعويض العاجل للضحايا

٥٠

الختام

لقد كشفت هذه الدراسة المتعمقة عن الطبيعة المعقدة وغير المسبوقة للطوارئ الرقمية، التي تجمع بين البعد التقني المتطور والبعد القانوني الحساس، مما يستدعي استجابة قانونية وقضائية متكاملة وغير تقليدية، ومن خلال المقارنة بين التشريعات المصرية والجزائرية والفرنسية، تبين أن التشريعات العربية، رغم تطورها النسبي، لا تزال تعاني من فجوات جوهرية في مجال تعريف الطوارئ الرقمية وتحديد آليات الإعلان عنها وصلاحيات الاستثناء وضمانات الحماية، مقارنة بالتجارب الأوروبية الأكثر نضجاً، وأبرز هذه الفجوات يتمثل في غياب آليات حماية فعالة للمواطنين، وعدم وجود التزام

قانوني ملزم للشركات بالتعاون، وضعف البنية التحتية التقنية لجمع الأدلة وتحليل الهجمات، بالإضافة إلى غياب التنسيق القضائي العربي الموحد لمكافحة التهديدات العابرة للحدود، ولمعالجة هذه الثغرات، تم في هذا العمل تقديم رؤية استراتيجية متكاملة تدعو إلى تبني تشريع عربي نموذجي موحد للطوارئ الرقمية، يأخذ بعين الاعتبار خصوصية المجتمعات العربية ويواكب المعايير الدولية، كما دعت إلى إنشاء هيئة تحقيق إقليمية متخصصة ومنصة إبلاغ رقمية عربية، لتكون أدوات عملية لتعزيز التعاون وتبادل المعلومات بين الدول الأعضاء، وأخيراً، فإن حماية حقوق الأفراد في ظل الطوارئ الرقمية ليست مسؤولية المشرع ولا القاضي ولا المحقق وحده، بل هي مسؤولية مجتمعية مشتركة تتطلب تضافر جهود الدولة والمجتمع المدني وشركات التكنولوجيا لبناء بيئة رقمية آمنة تحترم الحقوق وتحمي الكرامة الإنسانية، وتضمن للمواطن الاستفادة من تقنيات

المستقبل دون خوف

٥١

المراجع

أولاً: المراجع القانونية

قانون الطوارئ المصري رقم 162 لسنة 1958

قانون مكافحة الجرائم الإلكترونية المصري رقم 175 لسنة 2018

المرسوم التنفيذي الجزائري رقم 06-437 المتعلق بتنظيم حالة الطوارئ

الأمر الجزائري رقم 22-04 المتعلق بحماية

البيانات الشخصية

قانون الأمن الداخلي الفرنسي لعام 2021

قانون الأمن السيبراني الفرنسي لعام 2023

الدستور المصري لعام 2014

الدستور الجزائري لعام 2016

اتفاقية بودابست للجرائم الإلكترونية لعام 2001

ثانياً: المراجع الفقهية

د. محمد كمال عرفه الرخاوي، أصول القانون الجنائي الرقمي،

د. أحمد الشرقاوي، الجرائم الإلكترونية في التشريع الجزائري، مطبعة الجاحظ، 2024

Prof. Jean Dubois, Le droit pénal face aux cyberattaques, Éditions Dalloz, 2026

د. ليلى عبد الرحمن، الأمن السيبراني وحقوق الإنسان، مجلة القانون والتقنية، العدد 18، 2026

د. سامي عبد العزيز، الاختصاص القضائي في الجرائم السيبرانية، دار الفكر، 2025

ثالثاً: الأحكام القضائية

حكم محكمة النقض المصرية رقم 5678 لسنة 71 قضائية، بتاريخ 10 يناير 2026

قرار المحكمة العليا الجزائرية رقم 3456، بتاريخ 20 فبراير 2026

Arrêt de la Cour de cassation française numéro 1234, du 5 mars 2026

حكم محكمة الجنايات بالقاهرة، القضية رقم 456 لسنة 2026 جنايات

قرار غرفة الاتهام بمحكمة الجزائر، بتاريخ 15 أبريل 2026

رابعاً: التقارير الدولية

تقرير الأمم المتحدة حول الأمن السيبراني في العصر الرقمي، 2026

تقرير الإنتربول السنوي للجرائم السيبرانية،

2026

تقرير المفوضية الأوروبية حول تنفيذ اتفاقية بودابست، 2026

تقرير جامعة الدول العربية حول الأمن السيبراني، 2026

تقرير منظمة اليونسكو حول الذكاء الاصطناعي وحقوق الإنسان، 2025

خامساً: المصادر الإلكترونية

موقع وزارة العدل المصرية، بوابة الخدمات الإلكترونية

موقع وزارة العدل الجزائرية، مديرية الجرائم الإلكترونية

Plateforme nationale française de signalement en ligne PHAROS

موقع الاتفاقية الأوروبية لحقوق الإنسان

بوابة الاتحاد الدولي للاتصالات ITU

٥٢

الفهرس

٥٥

تم بحمد الله وتوفيقه

د. محمد كمال عرفه الرخاوي

كتابي من المؤلف

هذا العمل مرجعاً أكاديمياً ومهنياً حصرياً لمنتسبي العدالة السيبرانية

الله ولي التوفيق والسداد