جمهورية مصر العربية
رئيس الوزراء

قرار رئيس مجلس الوزراء
رقم (١٦٣٩) لسنة ٢٠٢٠
بإصدار اللائحة التنفيذية للقانون رقم ١٧٥ لسنة ٢٠١٨
بشأن مكافحة جرائم تقنية المعلومات

رئيس مجلس الوزراء

بعد الاطلاع على الدستور؛

وعلى قانون العقوبات ؛
وعلى القانون المدني ؛
وعلى قانون الإجراءات الجنائية ؛
وعلى القانون رقم ٩٦ لسنة ١٩٥٢ بشأن تنظيم الخبرة امام جهات القضاء ؛
وعلى قانون القضاء العسكري الصادر بالقانون رقم ٢٥ لسنة ١٩٦٦؛
وعلى قانون المرافعات المدنية والتجارية ؛
وعلى قانون الاثبات في المواد المدنية والتجارية ؛
وعلى قانون الطفل الصادر بالقانون رقم ١٢ لسنة ١٩٩٦؛
وعلى قانون التجارة الصادر بالقانون رقم ١٧ لسنة ١٩٩٩؛
وعلى قانون حماية حقوق الملكية الفكرية الصادر بالقانون رقم ٨٢ لسنة ٢٠٠٢؛
وعلى قانون تنظيم الاتصالات الصادر بالقانون رقم ١٠ لسنة ٢٠٠٣؛
وعلى قانون البنك المركزي والجهاز المصرفي والنقد الصادر بالقانون رقم ٨٨ لسنة ٢٠٠٣؛
وعلى قانون تنظيم التوقيع الإلكتروني الصادر بالقانون رقم ١٥ لسنة ٢٠٠٤؛
وعلى قانون حماية المنافسة ومنع الممارسات الاحتكارية الصادر بالقانون رقم ٣ لسنة ٢٠٠٥؛
وعلى قانون تنظيم خدمات النقل البري للركاب باستخدام تكنولوجيا المعلومات الصادر بالقانون رقم٨٧ لسنة ٢٠١٨؛
وعلى قانون مكافحة جرائم تقنية المعلومات الصادر بالقانون رقم ١٧٥ لسنة ٢٠١٨؛
وعلى قانون حماية المستهلك الصادر بالقانون رقم ١٨١ لسنة ٢٠١٨؛
وبناءً على ما ارتآه مجلس الدولة ؛

قرر

(المادة الأولى)

يُعمل بأحكام اللائحة التنفيذية المرافقة في شأن قانون مكافحة جرائم تقنية المعلومات المشار إليه.

(المادة الثانية)

يُنشر هذا القرار في الجريدة الرسمية ويعمل به من اليوم التالي لتاريخ نشره.

رئيس مجلس الوزراء

(دكتور/مصطفي كمال مدبولي)

صدر برئاسة مجلس الوزراء في ٨ المحـــــرم سنة ١٤٤٢هـ
الموافق ٢٧ أغسطـــس سنة ٢٠٢٠م

صورة مرسلة إلى السيد / جميع السادة الوزراء

رئيس
هيئة مستشاري مجلس الوزراء

(المستشار/ سيد الشاذلي)

جمهورية مصر العربية
مجلس الوزراء

المادة (١)

في تطبيق احكام هذه اللائحة يقصد بالكلمات والعبارات التالية المعنى المبين قرين كل منها:

- الجهاز : الجهاز القومي لتنظيم الاتصالات.
- التشفير Encryption: منظومة تقنية حسابية تستخدم مفاتيح خاصة لمعالجة وتحويل البيانات والمعلومات المقروءة الكترونياً بحيث تمنع استخلاص هذه البيانات والمعلومات إلا عن طريق استخدام مفتاح أو مفاتيح فك الشفرة.
- مفتاح التشفير Encryption Key: أرقام أو رموز أو حروف ذات طول محدد تستخدم في عمليات التشفير وفك التشفير. ويستخدم نفس المفتاح في التشفير وفك التشفير ويسمى التشفير المتماثل، ويجب الحفاظ على سرية المفتاح. ويستخدم زوج من المفاتيح مترابطين بعلاقة رياضية بحيث يستخدم أحدهما في التشفير والآخر في فك التشفير ويسمى التشفير غير المتماثل، ويجب الحفاظ على سرية أحد المفاتيح بينما يعلن عن الآخر بشروط ومعايير محددة.
- البنية التحتية المعلوماتية الحرجة Critical Information Infrastructure: مجموعة أنظمة أو شبكات أو أصول معلوماتية أساسية يؤدى الكشف عن تفاصيلاتها تعطيلها أو تغيير طريقة عملها بطريقة غير مشروعة، أو الدخول غير المصرح به عليها، أو الدخول أو الوصول بشكل غير قانوني للبيانات والمعلومات التي تحفظها أو تعالجها، أو يؤدى القيام بأي فعل غير مشروع أخر بها إلى التأثير على توافر خدمات الدولة ومرافقها الأساسية أو خسائر اقتصادية أو اجتماعية كبيرة على المستوى الوطني. ويعد من البنية التحتية المعلوماتية الحرجة على الأخص ما يستخدم في الطاقة الكهربائية، الغاز الطبيعي والبترول، الاتصالات، والجهات المالية والبنوك، والصناعات المختلفة، والنقل والمواصلات والطيران المدني، والتعليم والبحث العلمي، والبث الإذاعي والتليفزيوني، ومحطات مياه الشرب والصرف الصحي والموارد المائية، والصحة، الخدمات الحكومية وخدمات الإغاثة وخدمات الطوارئ، وغيرها من مرافق المعلومات والاتصالات التي قد تؤثر على الأمن القومي أو الاقتصاد القومي والمصلحة العامة وما في حكمها.
- نظام التحكم الصناعي: حاسب أو مجموعة حواسب متصلة ببعضها البعض، وبالمعدات المتحكم بها وأدوات الاتصال المتبادل بينهم رقمية Digital أو تناظرية Analog ، أو غيرها بما في ذلك الحساسات والمنفذات Actuator لتشغيل هذه المعدات والتحكم بها منطقياً طبقاً للصناعة المعنية، أو الاعمال المطلوبة في مكان واحد أو موزعة في أماكن متقاربة أو موزعة جغرافياً مع اتصل النظام بالإنترنت أو بغيره من الأنظمة المماثلة أو غير المماثلة أو استقلاله وعدم اتصاله بما عداه مع تراكم مستوى التحكم أو عدم تراكمه.
- نقاط الضعف Vulnerabilities: خلل أو ثغرة في نظام تشغيل أو تطبيقات أو شبكات المعلومات أو العمليات أو السياسات الخاصة بتأمين المعلومات أو في بيئة تقنية المعلومات او الاتصالات والتي يمكن استغلالها في عمليات الاختراق أو الهجوم أو الاتلاف أو التجسس أو أي عمل غير مشروع.

AR

المادة (٢)

يلتزم مقدمو خدمات تقنيات المعلومات باتخاذ الإجراءات التقنية والتنظيمية التالية تنفيذا للبندين (٢و٣) من الفقرة أولا من المادة رقم (٢) من القانون:-

١- تشفير البيانات والمعلومات بما يحافظ على سريتها، وعدم اختراقها باستخدام نظام تشفير قياسي متماثل أو غير متماثل لا يقل في تأمينه عن Advanced Encryption Standard (ASE-128) بمفتاح شفرة لا يقل عن ١٢٨ بت، مع مسئوليته بالحفاظ على سرية وأمان مفتاح التشفير.

٢- تنصيب واستخدام نظم وبرامج ومعدات مكافحة البرمجيات والهجمات الخبيثة والتأكد من صلاحيتها وتحديثها.

٣- استخدام بروتوكولات آمنة، مثل بروتوكول نقل النص التشعبي المؤمن HTTPS.

٤- وضع صلاحيات بالشبكات والملفات وقواعد البيانات وتحديد المسئولين، لضمان حماية الوصول المنطقي Logical Access إلى الأصول المعلوماتية والتقنية لمنع الوصول غير المصرح به.

٥- إعداد قائمة بالأجهزة والمعدات وأرقامها المميزة والمسلسلة وطرازاتها وكذا بيان بالنظم والبرامج والتطبيقات وقواعد البيانات المستخدمة ومواصفاتها.

٦- تطبيق أفضل الممارسات والضوابط عند اختيار مواصفات كلمات السر أو المرور وفقا للملحق رقم (١) المرفق باللائحة التنفيذية.

٧- توثيق إجراءات التنصيب والتشغيل الخاصة بالأنظمة.

٨- ضمان تنفيذ وتشغيل وصيانة الانظمة وإلزام الأطراف المتعاقد معها بإبرام اتفاقيات تحدد مستوى تقديم الخدمة مع الجهة وحدود مسئولية كل جهة.

٩- إجراء التحديثات الخاصة بالنظم والبرامج والتطبيقات بشكل دوري، وإتمام الاختبارات اللازمة قبل إجراء التحديثات.

١٠- إجراء اختبار سنوي للكشف عن الاختراقات أو المخاطر الأمنية.

١١- استخدام معدات وأجهزة ونظم وبرمجيات الجدران النارية (NGFW-UTM-Firewalls) لحماية الشبكات والنظم.

المادة (٣)

يلتزم مقدمو خدمات تقنية المعلومات والاتصالات التي تمتلك أو تدير أو تشغل البنية التحتية المعلوماتية الحرجة المخاطبين بأحكام هذا القانون، باتخاذ الإجراءات التقنية والتنظيمية التالية تنفيذاً للبندين (٢و٣) من الفقرة أولا من المادة رقم (٢) من القانون:-

١- إعداد سياسة أمن معلومات واعتمادها من الإدارة العليا للبنية التحتية المعلوماتية الحرجة وضمان مراجعتها كل عام لضمان استمرار ملائمة وكفاية وفاعلية تلك السياسة. على أن تتضمن تلك السياسة متطلبات الأجهزة والجهات الرقابية والتنظيمية المختصة بالبنية التحتية المعلوماتية الحرجة، والمتطلبات القانونية، والمتطلبات الخاصة بالموارد البشرية.

جمهورية مصر العربية
رئيس الوزراء

٢- ضمان التأكد من الامتثال لما ورد بهذا القانون ولائحته والقرارات التنفيذية ذات الصلة من التزامات تقنية أو تنظيمية.

٣- تشفير البيانات والمعلومات بما يحافظ على سريتها، وعدم اختراقها باستخدام نظام تشفير قياسي متماثل أو غير متماثل لا يقل تأمينه عن Advanced Encryption Standard (AES-256) بمفتاح شفرة لا يقل عن ٢٥٦ بت يتم توليده باستخدام نظام عشوائي آمن. واستخدام نظام إدارة مفاتيح تشفير قياسي للحفاظ على سريتها ودورة حياتها ومستويات استخدامها في التطبيقات المختلفة.

٤- استخدام شهادات تصديق الكرتوني صادرة من جهة من جهات إصدار شهادات التوقيع الالكتروني المعترف بها في جمهورية مصر العربية وبضوابط قانون تنظيم التوقيع الالكتروني ولائحته التنفيذية، وذلك لكافة المستخدمين لأنظمة المعلومات الخاصة بالبنية المعلوماتية التحتية الحرجة.

٥- منع الوصول المادي لغير المخول أو المصرح لهم الدخول أو الوصول لمقار وأجهزة ومعدات أنظمة البنية التحتية المعلوماتية الحرجة.

٦- استخدام ضوابط نفاذ قوية Strong Authentication وفعالة من خلال فئتين أو أكثر من فئات التوثق Multi-factor Authentication وبحسب مستوى المخاطر، بما يضمن تحديد المسئولية وعدم الانكار.

٧- توثيق إجراءات التنصيب والتشغيل الخاصة بنظم البنية التحتية المعلوماتية الحرجة واتاحتها للمستخدمين المخول لهم ذ لك عند حاجتهم إليها، وإلزام الموردين بتزويد الجهة بكامل الوثائق الخاصة بالإجراءات التشغيلية.

٨- ضمان تنفيذ وتشغيل وصيانة أنظمة البنية التحتية المعلوماتية الحرجة وإلزام الأطراف المتعاقد معها بإبرام اتفاقيات تحدد مستوى تقديم الخدمة مع الجهة.

٩- تنصيب واستخدام نظم وبرامج ومعدات المكافحة والحماية من البرمجيات والهجمات الخبيثة، والكشف عنها والتأكد من صلاحيتها وتحديثها.

١٠-إجراء التحديثات الخاصة بالنظم والبرامج والتطبيقات بشكل دوري. مع الأخذ في الاعتبار ضوابط التعامل مع إجراء التحديثات على أنظمة التحكم الصناعي مع عدم اتصالها المباشر بشبكة الانترنت، وإتمام الاختبارات اللازمة قبل إجراء التحديثات.

١١-إجراء مسح سنوي لأنظمة التحكم الصناعي للكشف عن الثغرات ونقاط الضعف واتخاذ الإجراءات اللازمة للتعامل معها.

١٢-إجراء اختبار سنوي للكشف عن الاختراقات أو المخاطر الأمنية وتثبيت أجهزة المنع والكشف عن الاختراقات.

١٣-اتخاذ الإجراءات الملائمة للتعامل مع الثغرات الفنية للأجهزة وللنظم والبرامج والتطبيقات عند العلم بها.

١٤-إجراء عمليات أخذ نسخ احتياطية شهرية للبيانات والمعلومات، والاحتفاظ بها وتخزينها مشفرة في موقع آخر.

١٥-استخدام معدات وأجهزة ونظم وبرمجيات الجدران النارية (NGFW- UTM- Firewalls) لحماية الشبكات والنظم.

١٦-استخدام بروتوكولات آمنة، مثل بروتوكول نقل النص التشعبي المؤمن HTTPS .

١٧-إعداد قائمة بالأجهزة والمعدات وأرقامها المميزة والمسلسلة وطرازاتها وكذا بيان بالنظم والبرامج والتطبيقات وقواعد البيانات المستخدمة ومواصفاتها.

١٨-تحديد مسئوليات الإدارة العليا ومسئولي تكنولوجيا المعلومات وأمن المعلومات بشكل واضح وصلاحيات وسلطات وواجبات والتزامات كل منهم، مع ضرورة اتساق ذلك مع ما تقوم به إدارات الموارد البشرية وشئون العاملين من إعداد الهياكل، والتوصيف الوظيفي، والأنشطة التدريبية وغيرها من أنشطة وعمليات تلك الإدارات.

١٩-إبلاغ المركز الوطني للاستعداد لطوارئ الحاسب والشبكات بالجهاز عن أي حوادث أو اختراقات فور العلم بحدوثها.

٢٠-وضع خطة استمرارية العمل والبدائل المقترحة في حال حدوث أي مخاطر أو أزمات تتعلق بت قديم الخدمة أو انقطاعها، والقدرة على استعادة الخدمة والعمل في حال الكوارث، واختبار الخطة دورياً.

المادة (٤)

يُنشأ بالجهاز سجلان لقيد الخبراء، يقيد بأولهما الفنيون والتقنيون العاملون بالجهاز، ويقيد بالآخر الخبراء من الفنيين والتقنيين من غير العاملين به. ويتم القيد في السجل الأول الخاص بالعاملين بالجهاز بناءاً على القواعد والشروط والإجراءات الآتية:-

١- أن يكون حاصلا على مؤهل علمي أو فني أو تقني يتناسب ومجال الخبرة.

٢-أن يكون قد أمضى عام على الأقل في عمله بالجهاز.

٣-ان يجتاز الاختبارات الفنية التي يجريها الجهاز للمتقدم.

المادة (٥)

يُقيد الخبراء من الفنيين والتقنيين من غير العاملين بالجهاز بالسجل الثاني للخبراء طبقا للقواعد والشروط الآتية:

١- أن يكون مصرياً متمتعا بالأهلية المدنية الكاملة. ويجوز قيد الأجنبي على أن يتعهد كتابة بخضوعه للقوانين المصرية.

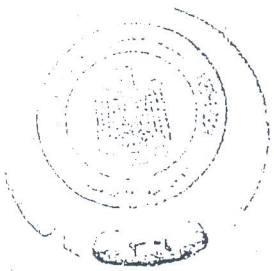
٢- ان يكون محمود السيرة حسن السمعة.

٣- الا يكون قد سبق الحكم عليه بحكم نهائي بالإدانة في جريمة مخلة بالشرف.

٤- ان يكون لدية سيرة ذاتية تتضمن خبرة عملية مناسبة.

٥- موافقة الجهات المعنية من جهات الامن القومي على القيد بالسجل.

ويترتب على تخلف أي شرط من الشروط السابقة الشطب من السجل بقرار من الجهاز.



مادة (٦)

يقوم الخبراء وفقاً للمادتين رقمي (١)، (١٠) من القانون بتنفيذ المهام الفنية والتقنية التي يتم تكليفهم بها من جهات التحقيق أو الجهات القضائية المختصة أو من الجهات المعنية بمكافحة جرائم تقنية المعلومات بشأن الجرائم موضوع هذا القانون.

مادة (٧)

يُراعى الجهاز الحفاظ على سرية البيانات الواردة بسجلات قيد الخبراء وعدم الإفصاح عنها إلا بموجب أمر قضائي.

مادة (٨)

يتعين على من يرغب في قيد اسمه في السجل الثاني للخبراء أن يتقدم للرئيس التنفيذي للجهاز بطلب كتابي بذلك موضحاً فيه التخصص الذي يرغب العمل فيه كخبير، وأن يرفق بالطلب صور الشهادات والمستندات المؤيدة لطلبه.

ويمكن للجهاز أن يطلب منه خلال ثلاثون يوماً من تاريخ تقديم الطلب معلومات إضافية قبل الفصل في الطلب، ويعتبر عدم الرد على الطلب لمدة ستين يوماً من تاريخ تقديمه رفضاً له. وفي حال رفض الجهاز الطلب، يحق للمتقدم التظلم بالإجراءات المقررة قانوناً.

المادة (٩)

تحوز الأدلة الرقمية ذات القيمة والحجية للأدلة الجنائية المادية في الإثبات الجنائي إذا توافرت فيها الشروط والضوابط الآتية:-

١- أن تتم عملية جمع أو الحصول أو استخراج أو استنباط الأدلة الرقمية محل الواقعة باستخدام التقنيات التي تضمن عدم تغيير أو تحديث أو محو أو تحريف للكتابة أو البيانات والمعلومات، أو أي تغيير أو تحديث أو إتلاف للأجهزة أو المعدات أو البيانات والمعلومات، أو أنظمة المعلومات أو البرامج أو الدعامات الالكترونية وغيرها. ومنها على الأخص تقنية Write Blocker، Digital Images، Hash وغيرها من التقنيات المماثلة.

٢- أن تكون الأدلة الرقمية ذات صلة بالواقعة وفي إطار الموضوع المطلوب إثباته أو نفيه، وفقا لنطاق قرار جهة التحقيق أو المحكمة المختصة.

٣- أن يتم جمع الدليل الرقمي واستخراجه وحفظه وتحريزه بمعرفة مأموري الضبط القضائي المخول لهم التعامل في هذه النوعية من الأدلة، أو الخبراء أو المتخصصين المنتدبين من جهات التحقيق أو المحاكمة، على أن يبين في محاضر الضبط، أو التقارير الفنية على نوع ومواصفات البرامج والأدوات والأجهزة والمعدات التي تم استخدمها، مع توثيق كود وخوارزم Hash الناتج عن استخراج نسخ مماثلة ومطابقة للأصل من الدليل الرقمي بمحضر الضبط أو تقرير الفحص الفني مع ضمان استمرار الحفاظ على الأصل دون عبث به.

٤- في حالة تعذر فحص نسخة الدليل الرقمي وعدم إمكانية التحفظ على الأجهزة محل الفحص لأي سبب يتم فحص الأصل ويثبت ذلك كله في محضر الضبط أو تقرير الفحص والتحليل.

٥- أن يتم توثيق الأدلة الرقمية بمحضر إجراءات من قبل المختص قبل عمليات الفحص والتحليل له وكذا توثيق مكان ضبطه ومكان حفظه ومكان التعامل معه ومواصفاته.

المادة (١٠)

يتم توصيف وتوثيق الدليل الرقمي من خلال طباعة نسخ من الملفات المخزن عليها أو تصويرها بأي وسيلة مرئية أو رقمية، واعتمادها من الأشخاص القائمين على جمع أو استخراج أو الحصول أو التحليل للأدلة الرقمية، مع تدوين البيانات التالية على كل منها:

١- تاريخ ووقت الطباعة والتصوير.
٢- أسم وتوقيع الشخص الذي قام بالطباعة والتصوير.
٣- أسم أو نوع نظام التشغيل ورقم الاصدار الخاص به.
٤- أسم البرنامج ونوع الاصدار أو الأوامر المستعملة لإعداد النسخ.
٥- البيانات والمعلومات الخاصة بمحتوى الدليل المضبوط.
٦- بيانات الأجهزة والمعدات والبرامج والأدوات المستخدمة.

المادة (١١)

يلتزم كل مسئول عن إدارة موقع أو حساب خاص أو بريد إلكتروني أو نظام معلوماتي سواء كان شخصا طبيعيا أو اعتبارياً وفقا للمادة رقم (٢٩) من القانون، باتخاذ التدابير والاحتياطات التأمينية الفنية اللازمة وفقا للالتزامات الواردة في المادة رقم (٣) من هذه اللائحة بالنسبة لمديرو مواقع مقدمي خدمات تقنية المعلومات.

كما يلتزم مديرو مواقع مقدمي خدمات تقنية المعلومات والاتصالات التي تمتلك أو تدير أو تشغل البنية التحتية المعلوماتية الحرجة بالالتزامات الواردة في المادة رقم (٣) من هذه اللائحة. ويلتزم الممثل القانوني ومسئول الإدارة الفعلية لمقدمي الخدمة بإثبات توفيره الإمكانيات التي تمكن مديرو المواقع من اتخاذ التدابير والاحتياطات التأمينية اللازمة لقيامه بعمله.

وفي جميع الأحوال يلتزم الممثل القانوني ومسئول الإدارة الفعلية ومدير الموقع لدى أي مقدم خدمة بإتاحة مفاتيح التشفير الخاصة به للمحكمة المختصة أو لجهات التحقيق المختصة في حال وجود تحقيق في إحدى الشكاوى أو المحاضر أو الدعاوى عند طلبها رسمياً من تلك الجهات.

المادة (١٢)

يشترط لاعتماد الجهاز إقرار المجني عليه بالصلح طبقا للمادة رقم ٤٢ من القانون، في الجرائم المنصوص عليها في المواد ١٤، ١٧، ١٨، ٢٣ استيفاء وتقديم ما يلي:

١- شهادة صادرة من النيابة أو المحكمة المختصة بحسب الأحوال بالقيد والوصف للجريمة محل الصلح.
٢- صورة طبق الأصل من المحضر أو الوثيقة التي أثبت فيها الصلح بين المتهم والمجني أو وكيله الخاص أو خلفه العام أمام النيابة أو المحكمة المختصة والمتضمنة إقرار المجني عليه بهذا الصلح.
٣- شهادة صادرة من النيابة المختصة تفيد عدم صدور حكم نهائي في الدعوى الجنائية.
٤- طلب باسم الرئيس التنفيذي للجهاز لاعتماد المحضر أو الوثيقة المتضمنة إقرار المجني عليه بالصلح يقدم من المتهم أو من وكيله أو من خلفه العام.

المادة (١٣)

يكون تصالح المتهم طبقا للمادة رقم ٤٢ من القانون، في الجرائم المنصوص عليها بالمادتين ٢٩، ٣٥ من القانون من خلال الجهاز باستيفاء وتقديم ما يلي:-

- شهادة صادرة من النيابة أو المحكمة المختصة بحسب الأحوال بالقيد والوصف للجريمة موضوع التصالح.
- شهادة صادرة من النيابة المختصة تفيد عدم صدور حكم نهائي في موضوع الجريمة محل طلب التصالح.
- أن يقدم المتهم الراغب في التصالح أو وكيله قبل رفع الدعوى الجنائية الإيصال الدال على سداده مبلغاً يعادل ضعف الحد الأقصى للغرامة المقررة للجريمة.
- أن يقدم المتهم الراغب في التصالح أو وكيله بعد رفع الدعوى الجنائية الإيصال الدال على سداده ثلثي الحد الأقصى للغرامة المقررة للجريمة أو قيمة الحد الأدنى للغرامة أيهما أكثر قبل صدور حكم نهائي في الموضوع.