**جريمة الاعتداء علي الأنظمة المعلوماتية الخاصة بالدولة**

**دراسة مقارنة بين القانون المصري والقانون الأمريكي في ضوء قانون الاحتيال وإساءة استخدام الحواسيب الأمريكي وقانون مكافحة جرائم تقنية المعلومات المصري رقم 175 لسنة 2018**

**د/ محمود عبد الغني فريد جاد المولي**

**مدرس القانون الجنائي – كلية الحقوق جامعة بنها**

**المجلة القانونية ( دورية علمية نصف سنوية ، محكمة ، ترقيم دولي**

 **2537-0758 - تصدر عن كلية الحقوق جامعة القاهرة فرع الخرطوم) العدد السابع**

**المجلدالثامن – مايو 2020 .**

**مستخلص الدراسة باللغة العربية**

 تعد الأنظمة المعلوماتية الخاصة بالدولة بالنظر لما تحويه من معلومات وبيانات غاية في الأهمية ، ولا سيما إذا كانت تلك المعلومات ذات صلة بالأمن القومي للدولة من أهم الأمور التي يجب علي المشرع حمايتها بنصوص تشريعية تجرم المساس بها بأي شكل من الأشكال ، وسوف نناقش الحماية الجنائية للأنظمة المعلوماتية الخاصة بالدولة في القانونين المصري والأمريكي :

**(1) الحماية الجنائية للأنظمة المعلوماتية الخاصة بالدولة في القانون الأمريكي :** قانون الاحتيال وإساءة استخدام الحواسيب (CFAA) Computer Fraud and Abuse Act ، الذي سنه الكونجرس في عام 1986 ، والذي عدل به المادة 18 U.S.C. § 1030 ، حاول الكونجرس من خلال هذا القانون تحقيق توازن مناسب بين مصلحة الحكومة الفيدرالية في الحماية من جرائم الكمبيوتر ومصالح وقدرات الولايات على حظر مثل هذه الجرائم والمعاقبة عليها ، وكما استمرت جرائم الكمبيوتر في النمو والتعقيد أدخل الكونجرس مزيدًا من التعديلات علي هذا القانون في أعوام 1988 ، 1989 ، 1990 ، 1994 ، 1996 ، 2001 ، 2002 ، 2008 ، 2020 ، ويتضمن هذا القانون في وقتنا الحالي سبعة صور من النشاط الإجرامي المحظور قانونا ، وهي الخاصة بالأجهزة والأنظمة الحاسوبية الحكومية والمنصوص عليها في المادة 1030 السالف الإشارة إليها ، وهي جريمة الحصول علي معلومات ذات صلة بالأمن القومي الأمريكي في المادة رقم 18 U.S.C. § 1030(a)(1) ، وجريمة الدخول إلي نظام حاسوبي والحصول علي معلومات تخص الملفات المالية للمؤسسات المالية في الدولة في المادة 18 U.S.C. § 1030(a)(2) ، وجريمة مجرد الاعتداء والدخول إلي جهاز حاسزبي حكومي ولو لم يتم الحصول علي أية معلومات في المادة رقم 18 U.S.C. § 1030(a)(3) ، وجريمة الاحتيال التي تشتمل على الوصول غير المصرح به إلى جهاز كمبيوتر حكومي أو جهاز كمبيوتر بنكي أو جهاز كمبيوتر مستخدم في مجال التجارة بين الولايات أو التجارة الخارجية أو يؤثر عليها في المادة 18 U.S.C. § 1030(a)(4) ، وجريمة إتلاف جهاز كمبيوتر حكومي أو جهاز كمبيوتر بنكي أو جهاز كمبيوتر مستخدم في مجال التجارة بين الولايات أو التجارة الخارجية أو يؤثر عليها في المادة 18 U.S.C. § 1030(a)(5) من خلال أي شكل من أشكال الهجوم السيبراني عبر الإنترنت ، أو التهديد بإتلاف هذه الأجهزة بموجب المادة رقم 18 U.S.C. § 1030(a)(7) ، وجريمة الاتجار بكلمات مرور لجهاز كمبيوتر حكومي وعندما يؤثر هذا الاتجار على التجارة بين الولايات أو التجارة الخارجية في المادة رقم 18 U.S.C. § 1030(a)(6) .

**(2) الحماية الجنائية للأنظمة المعلوماتية الخاصة بالدولة في القانون المصري :** واجه المشرع المصري جرائم تقنية المعلومات في مرحلة زمنية متأخرة عن نظيره الأمريكي بإصدار قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018 ، وبخصوص الحماية الجنائية للأنظمة المعلوماتية الخاصة بالدولة نجد المشرع المصري قد تعرض لها في نصين فقط من نصوص القانون أنف الذكر ، وهما المادتين رقم (20) ورقم (21) .

 وبالإضافة إلي النصين السابقين الواردين في قانون مكافحة جرائم تقنية المعلومات ، فقد يكون النظام المعلوماتي الخاص بالحكومة مملوكا للقوات المسلحة أو لوزارة الدفاع ، وقد يحوي أسراراً عسكرية متعلقة بالأمن القومي فما مدي سريان هذين النصين ، وكذلك هل تنطبق النصوص التقليدية الواردة بالباب الأول من الكتاب الثاني من قانون العقوبات ( الجنايات والجنح المضرة بأمن الحكومة من جهة الخارج ) .

**مستخلص الدراسة باللغة الإنجليزية**

 The state's computer systems includes information and data are extremely important, especially if that information is related to the state's national security, one of the most important matters that the legislator must protect with legislative texts that criminalize harming it in any way.

 We will discuss the criminal protection of the state's computer systems in the Egyptian and American laws:

(1) criminal protection for the state’s computer system in American law :

The Computer Fraud and Abuse Act (CFAA) Enacted by Congress in 1986 , which was amended the Section 18 U.S.C. § 1030, through this act, Congress attempted to strike an appropriate balance between the federal government's interest in protecting against computer crime and the interests and capabilities of states to prohibit and punish such crimes, and as computer crime continued to grow and complex, Congress introduced further amendments to this act in 1988 ,1989, 1990, 1994, 1996, 2001, 2002, 2008, 2020, and this law includes at the present time seven forms of criminal activity that are prohibited by law, which are related to government computer systems and systems stipulated in Article 1030 mentioned above, which is the crime of obtaining Information relevant to US national security in Article 18 U.S.C. § 1030(a)(1), and the offense of accessing a computer system and obtaining information regarding the financial files of financial institutions in the country in Section 18 U.S.C. § 1030(a)(2), and the offense of mere assault and entering a government computer system even if no information is obtained in Section 18 U.S.C. § 1030(a)(3), and the offense of fraud involving unauthorized access to or affecting a government computer, a bank computer, or a computer used in interstate or foreign commerce in 18 U.S.C. § 1030(a)(4), and the offense of damaging or affecting a government computer, a bank computer, or a computer used in interstate or foreign commerce in Section 18 U.S.C. § 1030(a)(5) through any form of cyber-attack, or threat to damage such equipment under 18 U.S.C. § 1030(a)(7), the offense of trafficking in government computer passwords and when such trafficking affects interstate or foreign commerce in 18 U.S.C. § 1030(a)(6).

(2) the criminal protection for the state’s computer systems in The Egyptian law :

 The Egyptian legislator faced information technology crimes at a later stage in time than his American counterpart by issuing the Anti-Information Technology Crimes Law No. 175 of 2018, and regarding criminal protection for the state’s information systems, we find the Egyptian legislator has It was presented in only two texts of the aforementioned law, namely Articles No. (20) and No. (21).

 In addition to the two previous texts contained in the Law on Anti-Information Technology Crimes, the government’s computer systems may be owned by the armed forces or the Ministry of Defense, and it may contain military secrets related to national security. Penal Code (felonies and misdemeanors harmful to the security of the government from abroad) .