جامعة الأزهر
كلية الشريعة والقانون
بالقاهرة

مجلة الشريعة والقانون

مجلة علمية نصف سنوية محكمة
تعنى بالدراسات الشرعية والقانونية والقضائية

تصدرها
كلية الشريعة والقانون بالقاهرة
جامعة الأزهر

العدد الرابع والأربعون
نوفمبر ٢٠٢٤م

توجه جميع المراسلات باسم الأستاذ الدكتور: رئيس تحرير مجلة الشريعة والقانون

جمهورية مصر العربية - كلية الشريعة والقانون - القاهرة - الدراسة - شارع جوهر القائد

ت: ٢٥١٠٧٦٨٧

فاكس: ٢٥١٠٧٧٣٨

https://mawq.journals.ekb.eg/

جميع الآراء الواردة في هذه المجلة تعبر عن وجهة نظر أصحابها، ولا تعبر بالضرورة عن وجهة نظر المجلة وليست مسئولة عنها

رقم الإيـــداع

٢٠٢٤ / ١٨٠٥٣

الترقيم الدولي للطباعة

ISSN: 2812–4774

الترقيم الدولي الإلكتروني:

ISSN: 2812–5282

البعد الدولي لجرائم الذكاء الاصطناعي (A.I)
في ضوء التشريعات الجزائية المقارنة

International Dimension Of Artificial Intelligence (AI)
Crimes In Light Of Comparative Penal Legislation

إعداد

د. أحمد عبدالله عبدالعزيز الحبيب

أكاديمية سعد العبدالله للعلوم الأمنية- قسم القانون العام
دولة الكويت

البعد الدولي لجرائم الذكاء الاصطناعي (A.I)
في ضوء التشريعات الجزائية المقارنة

أحمد عبدالله عبدالعزيز الحبيب
قسم القانون العام، أكاديمية سعد العبدالله للعلوم الأمنية، دولة الكويت.
البريد الإلكتروني: **Bo7bib@gmail.com**

ملخص البحث :

تنبع أهمية هذه الدراسة من كونها تتناول الذكاء الاصطناعي (A.I) من زاوية الجانب السلبي منها والمتعلق بجرائم المعلوماتية وتأثيره على مكونات المجتمع. وأمام هذا الشكل الجديد من الإجرام لا تبدو قوانين العقوبات الوطنية في حالتها الراهنة كافية أو فعالة على النحو المطلوب.

وترتيبا على ما سبق يمكن للباحث صياغة المشكلة البحثية للدراسة الحالية على هيئة تساؤل رئيس كما يلي: **ما هي الآليات المختلفة للجوانب الإجرائية والتشريعية للضبط القانوني العربي والدولي حيال جرائم الذكاء الاصطناعي (A.I)؟**

توصيات الدراسة

١- ضرورة تقنين قواعد جديدة لمكافحة جرائم الذكاء الاصطناعي (A.I) ؛ تأخذ بعين الاعتبار الطبيعة الخاصة لهذه الجرائم ولاسيما فيما يتعلق بالإثبات في الدعاوى الناشئة عن هذه الجرائم ؛ سواء في ذلك الدعاوى الجنائية أو المدنية أو التأديبية. كما ينبغي تعديل قواعد الإجراءات الجنائية لتتلاءم مع هذه الجرائم.

٢- ضرورة التنسيق والتعاون الدولي قضائيا وإجرائيا لمكافحة جرائم الذكاء الاصطناعي (A.I).

٣- ضرورة تخصيص شرطة خاصة لمكافحة جرائم الذكاء الاصطناعي (A.I) ؛ وذلك من رجال الشرطة المدربين على كيفية التعامل مع أجهزة الحاسب الآلي (Computer) والإنترنت (Internet).

الكلمات المفتاحية: البعد الدولي، جرائم، الذكاء الاصطناعي، التشريعات المقارنة.

International dimension of artificial intelligence (AI) crimes in light of comparative penal legislation

Ahmed Abdullah Abdulaziz Al Habib
Public Law Department, Saad Al Abdullah Academy for Security Sciences, The State of Kuwait.
E-mail: Bo7bib@gmail.com

Abstract:

The importance of this study stems from the fact that it deals with artificial intelligence (AI) from the angle of the negative side of it and related to cybercrime and its impact on the components of society.

, the researcher can formulate the research problem of the current study in the form of a key question as follows: What are the different mechanisms of procedural and legislative aspects of Arab and international legal control against artificial intelligence (AI) crimes?

Study recommendations

1. The need to codify new rules to combat artificial intelligence (AI) crimes; Take into account the special nature of these offences, in particular as regards proof in proceedings arising from these offences; Both criminal, civil and disciplinary actions. The rules of criminal procedure should also be amended to accommodate such offences.
2. The need for international judicial and procedural coordination and cooperation in combating artificial intelligence (AI) crimes.
3. The need to allocate special police to combat artificial intelligence (AI) crimes; The police are trained in how to deal with computers and the Internet.

Keywords: International Dimension, Artificial Intelligence, Crimes, Comparative Legislation.

المبحث التمهيدي
الإطار العام للدراسة

مقدمـــة

يمكن التأكيد أنه بعيدا عن الاستخدامات الحميدة أو السلمية للكمبيوتر، يمكن القول بأن التطور المذهل فى مجال الذكاء الاصطناعي (A.I)، قد ترتب عليه نشوء جرائم ناتجة عن استخداماته المتعددة، وهذه الجرائم إما أن تقع على الحاسب الآلي ذاته، وإما أن تقع بواسطة الحاسب الآلي حيث يصبح أداة في يد الجاني يستخدمه لتحقيق أغراضه الإجرامية.

ونظرا لازدياد الجرائم المتعلقة بالذكاء الاصطناعي (A.I) شرعت الدول المتمدينة بوضع تشريعات جنائية خاصة لمكافحة جرائم الذكاء الاصطناعي (A.I) التي تعد ظاهرة مستحدثة علي علم الإجرام، ومن هذه الدول الولايات المتحدة الأمريكية وفرنسا وباقى دول الاتحاد الأوروبي الذي وضع اتفاقية حول جرائم الحاسب الآلي سنة ٢٠٠١م، والتي أوصت فيها الدول الأعضاء باتخاذ كافة الإجراءات التشريعية أو غيرها حسب الضرورة لجعل الدخول إلى جميع نظم الحاسب الآلي أو أي من أجزائه بدون وجه حق جريمة جنائية بحسب القانون المحلي، كما أوصت هذه الاتفاقية على مجموعة من المبادئ العامة المتعلقة بالتعاون الدولي في مجال الشئون الجنائية، وحددت كذلك الإجراءات المتعلقة بطلبات المساعدة المتبادلة بين الدول الأعضاء في غياب الاتفاقيات الدولية. وهكذا وجد العالم نفسه في قرية صغيرة، وأصبحت قرية المعلومات هذه محط أنظار جميع أصحاب المصالح المشروعة وغير المشروعة، وبدأ الذكاء الاصطناعي (A.I) يفرز آثارا شاملة على البنية الإدارية والاقتصادية والاجتماعية والسياسية،والثقافية ،والقانونية للدول ،ذلك أن كل إختراع علمي لابد أن يفتح آفاقا جديدة ويرتب آثارا ما كانت قائمة قبل وجوده وانتشاره، وهنا كان لابد للقانون أن يتدخل، كيف لا وهو المنظم بقواعده على اختلاف أنواعها، لجميع مناحى الحياة.

وتنبع أهمية هذه الدراسة من كونها تتناول الذكاء الاصطناعي (A.I) من زاوية الجانب السلبى منها والمتعلق بجرائم المعلوماتية وتأثيره على مكونات المجتمع. وأمام هذا الشكل الجديد من الإجرام لا تبدو قوانين العقوبات الوطنية في حالتها

الراهنة كافية أو فعالة على النحو المطلوب أو المرضي فنصوصها والنظريات والمبادئ القانونية التي تتضمنها أو تقف وراءها موروث بعضها من القرن ١٩. وإزاء ذلك كان لا بد من تكاتف الدول من أجل مكافحة هذا النوع المستحدث من الجرائم، التي لم تعد تتمركز في دولة معينة، ولا توجه لمجتمع بعينه بل أصبحت تعبر الحدود لتلحق الضرر بعدة دول ومجتمعات، مستغلة التطور الكبير للوسائل التقنية الحديثة في الاتصالات والمواصلات، وتعزيز التعاون بينها واتخاذ تدابير فعّالة للحد منها والقضاء عليها ومعاقبة مرتكبيها.

مشكلة الدراسة

يمكن للباحث التأكيد أن جرائم الذكاء الاصطناعي، هى ظاهرة إجرامية جديدة ومستجدة تقرع في جنباتها أجراس الخطر لتنبه مجتمعات العصر الراهن لحجم المخاطر وهول الخسائر الناجمة عن جريمة الذكاء الاصطناعي التي تستهدف الاعتداء على المعطيات بدلالتها التقنية الواسعة (بيانات ومعلومات وبرامج بكافة أنواعها). فجريمة الذكاء الاصطناعي جريمة تقنية تنشأ في الخفاء، توجه للنيل من الحق في المعلومات، وتطال اعتداءاتها معطيات الحاسب المخزنة والمعلومات المنقولة عبر نظم وشبكات المعلومات.

هذه الجرائم تهدد الأمن القومي والسيادة الوطنية، وتشيع فقدان الثقة بالتقنية وتهدد إبداع العقل البشري، لذا فإن إدراك ماهية جرائم الذكاء الاصطناعي، منوط بتحليل وجهة نظر الدارسين لتعريفها والاصطلاحات الدالة عليها واختيار أكثرها اتفاقًا مع الطبيعة الموضوعية لهذه الجرائم، واستظهار موضوعها وخصائصها ومخاطرها وحجم الخسائر الناجمة عنها وسمات مرتكبيها ودوافعهم. وترتيبا على ما سبق يمكن للباحث صياغة المشكلة البحثية للدراسة الحالية على هيئة تساؤل رئيس كما يلي:

ما هي الآليات المختلفة للجوانب الإجرائية والتشريعية للضبط القانوني العربي والدولي حيال جرائم الذكاء الاصطناعي (A.I)؟

تساؤلات الدراسة

تطرح الدراسة الحالية مجموعة من التساؤلات الفرعية التالية:

١) ما هي الأبعاد المختلفة لجرائم الذكاء الاصطناعي في الدول العربية والغربية؟

٢) ما أبرز المعوقات التشريعية والقانونية المتعلقة بجرائم الذكاء الاصطناعي؟

٣) ما هي تدابير الضبط القانوني العربي والدولي في مجال مكافحة جرائم الذكاء الاصطناعي؟

أهمية الدراسة

يمكن تحديد أهمية هذه الدراسة في ضوء الاعتبارات التالية:

١- حداثة موضوع الدراسة على المستوى العربي ، إذ يجد الباحث ندرة في الكتابات الأكاديمية العربية التي سعت للخوض في هذا الموضوع.

٢- يستمد هذا الموضوع أهميته من طبيعة هذه الجرائم ودورها، فهذه الجرائم تعد حديثة على المجتمع العربي، وتحتاج للمزيد من الاهتمام والدراسة.

٣- الوقوف على بعض الجوانب والنقاط المهمة والمؤثرة في جرائم الذكاء الاصطناعي، وعلاقتها بخلق عوالم جديدة من التحديات أمام القضاء العربي والعالمي.

٤- تمهيد الطريق أمام إجراء عدد من الدراسات التي تناولت الموضوعات المماثلة لموضوعنا هذا بصورة علمية وشاملة والتي تضيف المزيد من المتغيرات المؤثرة في هذه الدراسة، بما يسهم في تحقيق التراكم المعرفي والبحث.

منهاجية الدراسة

سعى الباحث إلى الاستفادة من بعض المناهج في دراسة موضوع البحث وذلك على النحو التالي :

١ – **المنهج القانوني**" يتم استخدام هذا المنهج وذلك من خلال معالجة وتحليل الأساليب والطرق والإجراءات التي تم اللجوء إليها في تطبيقات جرائم مرتبطة بالذكاء الاصطناعي (A.I) في البيئة السيبرانية الجديدة.

٢ – **المنهج المقارن**" تعتمد الدراسة على المنهج التحليلى المقارن فى محاولة لكشف الاتجاهات المختلفة لتشريعات الذكاء الاصطناعي (A.I) وتطوراتها فى ضوء مستجدات عالم الرقمنة الجديد.

بنية الدراسة

تم تقسيم الدراسة الحالية إلى أربعة مباحث رئيسة وذلك كما يلي:

المبحث الأول: الأحكام العامة لجرائم الذكاء الاصطناعي (A.I)..الماهية والنشأة والتطور

المبحث الثاني: تصنيف جـرائم الذكاء الاصطناعي

المبحث الثالث: المعوقات المرتبطة بالضبط التشريعي لجرائم الذكاء الاصطناعي (A.I)

المبحث الرابع: إجراءات الضبط التشريعي في مجال مكافحة جرائم الذكاء الاصطناعي (A.I)

المبحث الأول

الأحكام العامة لجرائم الذكاء الاصطناعي (A.I)..الماهية والنشأة والتطور

لقد أرجع الفقه الجنائي جرائم الحاسب الآلي (Computer) إلى العام ١٩٦٠[١].

وأما جرائم الذكاء الاصطناعي (A.I) فإنه يمكن القول إنها بدأت مع العام ١٩٨٨ وكانت أول الجرائم التي ترتبط عضوياً بالإنترنت (Internet) هي جرائم العدوان الفيروسي فيما هو معروف في التاريخ القانوني بجريمة دودة موريس المؤرخة واقعتها في ٢ الحرث / نوفمبر ١٩٨٨. ولا يزال الفقه والتشريع المقارن في حقيقة الأمر يستشعر الحرج في التمييز بين كل من جرائم الحاسب الآلي وبين تلك الناجمة عن استخدام الإنترنت (Internet) ، حتى إن تقرير الأمم المتحدة عن منع الجريمة عام ١٩٩٥ تبني الموقف المقارن المذكور هذا فصدر عنوان التقرير Computer crimes & other crimes related to computer

لذلك نجد أن تعريف جرائم الحاسب الآلي (Computer) في الفقه والتشريع يسوده اتجاه يجمع بين الجرائم التي تقع على الحاسب الآلي ذاته وتلك التي يكون الحاسب الآلي وسيلة ارتكابها، فهي لدي هذا الاتجاه تعرف بأنها "فعل غير مشروع يتورط نظام الحاسب الآلي (Computer) فيه، سواء كان الحاسب الآلي كآلة هو موضوع الجريمة أو كان الوسيلة إلى ارتكابها أو مستودع الدليل المرتبط بالجريمة". وهو تعريف مستمد من أكثر التعريفات شعبية لجرائم الحاسب الآلي (Computer) الذي قال به الأستاذ Donn Parker من حيث إن جرائم الحاسب الآلي (Computer) هي "جرائم تتطلب دراية ضرورية بالحاسب الآلي لكي يتم ارتكاب الجريمة بنجاح"[٢]. ولم تأت الاتفاقية الأوروبية للجريمة عبر العالم الافتراضي

---

(1) (SIEBER) Dr. Ulrich – Computer crimes & other crimes related to information technology rev. inter.de droit penal 1991 p. 1033.

(2) Voir site : remp (the royal candian mounted police) " computer crimes is any illegal act which involves a computer systems whether the computer is an obect of crime, an instrument used to commit a crime or a respsitory of evidence related to a crime". Available online in feb. 2000 at: http://www.rcmp.com (mak d. rasch – criminal law and the internet – the internet and association. Copyright © 1996 by the computer law association,

المؤرخة ٢٠٠١/١١/٢٣ على تعريف محدد للجريمة عبر الإنترنت (Internet)[١]، وإنما اعترفت بنوعية من الجرائم يمكن ارتكابها عبر الإنترنت .

أولا: ماهية الذكاء الاصطناعي (A.I)

لاشك أن تطبيقات الذكاء الاصطناعي (A.I) بأشكاله المختلفة ومراحله المتعددة تستمر في التطور والدخول في تطبيقات حياتنا اليومية شيئا فشيئاً، ويمكننا رؤية ذلك في طريقة تعامل هواتفنا مع الصور أو في برمجيات الذكاء الاصطناعي (A.I) به مثل تطبيق "Siri" الخاص بشركة Apple أو تطبيق "Bixby" الخاص بشركة سامسونج أو "Alexa" أو حتى "Google Search Voice" وغيرها الكثير، وأيضا الحواسيب الخاصة بالسيارات الحديثة التي تستخدم تطبيقات الذكاء الاصطناعي (A.I) لمعرفة الجو أو اكتشاف الطرق أو كمية الوقود المتبقية، أو حتى تطبيقات الذكاء الاصطناعي (A.I) في ألعاب الفيديو، كل هذه التطبيقات وغيرها الكثير والكثير تعد أمثلة للتقدم العالمي في مجال الذكاء الاصطناعي (A.I)[٢].

ومن الممكن تناول كلمتي الذكاء والاصطناعي في اللغة والاصطلاح كما يلي:

مفهوم الذكاء في اللغة والاصطلاح

الذَّكاءُ لغةً:

الذَّكاءُ: سرعةُ الفِطنةِ، من قَولِك: قَلبٌ ذَكيٌّ وصَبيٌّ ذَكيٌّ: إذا كان سريعَ الفِطنةِ، وقد ذَكِيَ -بالكَسرِ- يَذكَى ذَكًا. ويُقالُ: ذكا يذكو ذَكاءً، وذَكُوَ فهو ذَكيٌّ .

الذَّكاءُ اصطِلاحًا:

قال المُناويُّ: (الذَّكاءُ: سُرعةُ الإدراكِ، وحِدَّةُ الفَهمِ)[٣]

---

inc. p.6, donn parker of sri, is necessary for the successful commission of the offense.

(1) Convention on CyberCrime – Explanatory Report, adopted on 8 Nov. 2001

(٢) د. عبد الرازق مختار محمود، تطبيقات الذكاء الاصطناعي: مدخل لتطوير التعليم في ظل جائحة كوفيد ١٩، المجلة الدولية للبحوث في العلوم التربوية، المجلد٣، العدد٤، ٢٠٢٠ــ ، ص.٢٠٨

(٣) موقع الدرر السنية على الشبكة المعلوماتية https://dorar.net/alakhlaq/2268/%84%D8%A7%D8%AD%D8%A7 تاريخ الدخول ٢٠ نوفمبر ٢٠٢٤

الاصطناعي لغة

اِصطناعيّ: اسم منسوب إلى اصطناع وهو ما كان مصنوعًا، غير طبيعيّ حريرٌ/ وَرْدٌ اصطناعيّ[١]

الاصطناعي اصطلاحا

هو إحداث الفعل المصنوع من خلال جهد مبذول بغية الوصول إلى نتائج محددة

وبالنظر إلى تعريف الذكاء الاصطناعي (A.I) على أنه أتمتة قائمة على الارتباطات نتناول أدناه ثلاث وجهات نظر إضافية حول ما يشكل الذكاء الاصطناعي (A.I). سيجد مختصو التعليم أن وجهات النظر المختلفة هذه تنشأ في تسويق وظائف الذكاء الاصطناعي (A.I) ومن المهم فهمها عند تقييم أنظمة تكنولوجيا التعليم التي تتضمن الذكاء الاصطناعي (A.I). أحد القوائم المفيدة لمصطلحات الذكاء الاصطناعي (A.I) للتعليم هو قائمة مصطلحات الذكاء الاصطناعي (A.I) للمعلمين[٢]. وبالتالي فإن الذكاء الاصطناعي (A.I) ليس شيئا واحدا ولكنه مصطلح شامل لمجموعة متزايدة من قدرات النمذجة[٣]

ويمكن تتبع الوعي الثقافي الواسع بالذكاء الاصطناعي (A.I) وصولا إلى الفيلم المميز عام ١٩٦٨ "٢٠٠١: أوديسا الفضاء" - حيث يتحدث كمبيوتر "الإرشاد" المبرمج بالخوارزميات، أو اختصارا "HAL"، مع رائد الفضاء فرانك. حيث يساعد HAL فرانك في قيادة الرحلة عبر الفضاء، وهي وظيفة لا يستطيع فرانك القيام بها بمفرده. ومع ذلك، يذهب فرانك في النهاية خارج المركبة الفضائية، ويتولى HAL السيطرة، وهذا لا ينتهي بشكل جيد بالنسبة لفرانك. حيث يعرض HAL سلوكيات شبيهة بالإنسان مثل الإدراك والتحدث والتصرف. مثل جميع تطبيقات

---

(١) معجمم المعاني متاح على شبكة الانترنت https://www.almaany.com/ar/dict/ar-a؟
تاريخ الدخول ٢٠ نوفمبر ٢٠٢٤

(2)Megel .A. Cardona, Artificial Intelligence and Education future, USA, Office of Education Technology, May 2023, P.13

(3)Regona, Massimo & Yigitcanlar, Tan & Xia, Bo & Li, R.Y.M. (2022). Opportunities and adoption challenges of Al in the construction industry: A PRISMA review. Journal of Open Innovation Technology Market and Complexity, 8(45). https://doi.org/10.3390/joitmc8010045

الذكاء الاصطناعي (A.I)، يمكن أن يساعد HAL البشر، ولكنه يقدم أيضا مخاطر غير متوقعة - خاصة وأن طرق إدراك الذكاء الاصطناعي (A.I) وحدود تلك الطرق مختلفة عن البشر.

فكرة "الشبيه بالإنسان مفيدة لأنها يمكن أن تكون اختصارا لفكرة أن أجهزة الحاسب الآلي لديها الآن قدرات مختلفة تماما عن قدرات تطبيقات تكنولوجيا التعليم المبكرة. ستكون التطبيقات التعليمية قادرة على التحدث مع الطلاب والمعلمين والمشاركة في تجربة كيفية تطور الأنشطة في الفصول الدراسية، واتخاذ الإجراءات التي تؤثر على الطلاب والمعلمين على نطاق واسع. ستكون هناك فرص للقيام بالأشياء بشكل أفضل بكثير مما نقوم به اليوم ومخاطر يجب توقعها ومعالجتها.

ومع ذلك، فإن اختزال "الشبيه بالإنسان" ليس مفيدا دائما، لأن الذكاء الاصطناعي (A.I) يعالج المعلومات بشكل مختلف عن كيفية معالجة الأشخاص للمعلومات عندما نتغاضى عن الاختلافات بين الناس وأجهزة الحاسب الآلي، فقد نضع سياسات ذكاء اصطناعي في التعليم تخطئ الهدف[١].

كذلك فإن الذكاء الاصطناعي (A.I) هو بمنزلة نظرة خوارزمية تسعى لتحقيق هدف "أي طريقة حسابية يتم إجراؤها للعمل بشكل مستقل نحو هدف تعتمد على الاستنتاجات من نظريات أو على الأنماط في البيانات"[٢].

ويؤكد هذا التعريف على أن أنظمة وأدوات الذكاء الاصطناعي (A.I) تحدد الأنماط وتختار الإجراءات لتحقيق لذلك معين. سيتم استخدام هذه القدرات في التعرف على الأنماط والتوصيات الآلية بطرق تؤثر على العملية التعليمية، بما في ذلك تعلم الطلاب واتخاذ القرارات التعليمية للمعلمين على سبيل المثال، قد تتعرف أنظمة التعلم الشخصية اليوم على علامات أن الطالب يعاني وقد توصي بتسلسل تعليمي بديل. سيتم توسيع نطاق التعرف على الأنماط والتوصيات الآلية.

---

(1) Megel .A. Cardona, Artificial Intelligence and Education future, Op, Cit, P.13

(2)Friedman, L., Blair Black, N., Walker, E., & Roschelle, J. (November 8, 2021) Safe Al in education needs you. Association of Computing Machinery blog, https://cacm.acm.org/blogs/blog-cacm/256657-safe-ai-in-education-needs-you/ fulltext

وعلى الرغم من أن هذه النظرة يمكن أن تكون مفيدة، إلا أنها قد تكون مضللة. تتضمن النظرة الإنسانية للوكالة والسعي لتحقيق الأهداف والتفكير قدراتنا البشرية على فهم سياقات متعددة. على سبيل المثال، قد يرى المعلم ثلاثة طلاب يرتكب كل منهم نفس الخطأ الرياضي ولكنه يدرك أن أحد الطلاب لديه برنامج تعليمي فردي لمعالجة مشكلات الرؤية وآخر يفهم مفهوما رياضيا والثالث يعاني للتو من تفاعل محبط في الملعب ؛ وبالتالي فإن نفس القرار التعليمي غير مناسب. ومع ذلك، غالبا ما تفتقر أنظمة الذكاء الاصطناعي (A.I) إلى البيانات والحكم لتضمين السياق بشكل مناسب أثناء اكتشافها للأنماط وأتمتة القرارات. علاوة على ذلك، تظهر دراسات الحالة أن التكنولوجيا لديها القدرة على الخروج بسرعة عن مسارها من آمنة إلى غير آمنة أو من فعالة إلى غير فعالة عندما يتغير السياق ولو قليلا. لهذا السبب ولأسباب أخرى، يمكن للأشخاص المشاركة في تحديد الأهداف وتحليل الأنماط واتخاذ القرارات[١].

والذكاء المعزز هو نمط تصميم يعتمد على الإنسان في نموذج شراكة بين البشر والذكاء الاصطناعي (AI) (A.I) يعملان معا لتعزيز الأداء المعرفي، بما في ذلك التعلم وصنع القرارات والتجارب الجديدة.[٢]"

وتشبه نماذج الذكاء الاصطناعي (A.I) النماذج المالية: تقريب مفيد للواقع لتحديد الأنماط أو إجراء التنبؤات أو تحليل القرارات البديلة. في منهج رياضيات نموذجي بالمدرسة المتوسطة يستخدم الطلاب نموذجا رياضيا لتحليل خطتي شراء هاتف خلوي وأيهما أفضل. يستخدم المخططون الماليون هذا النوع من النماذج لتقديم إرشادات حول محفظة التقاعد في جوهره الذكاء الاصطناعي (A.I) هو مجموعة أدوات رياضية متقدمة للغاية لبناء النماذج واستخدامها في الواقع، وفي روبوتات المحادثة المعروفة، تتم كتابة المقالات المعقدة كلمة بكلمة في كل مرة حيث يتنبأ نموذج الذكاء الاصطناعي (A.I) الأساس بالكلمات التالية التي من المحتمل أن تتبع النص المكتوب حتى الآن.

(1)Russell, S. (2019). Human compatible: Artificial intelligence and the problem of control. Viking. ISBN 978-0-525-55861-3.
(2)Gartner (n.d.) Gartner glossary: Augmented intelligence. Gartner: https://www. gartner.com/en/informationtechnology/glossary/augmented-intelligence

تستخدم روبوتات محادثة الذكاء الاصطناعي (A.I) نموذجا إحصائيا كبيرا جدا لكلمة واحدة محتملة في كل مرة، وبالتالي نحصل على كتابة مقالات متماسكة بشكل مدهش[١].

ثانيا: : تطور البنية التشريعية لجرائم الذكاء الاصطناعي (A.I)

لقد توسعت إدارة العدل الأمريكية في ربط الحاسب الآلي (Computer) بتقنيته فذهبت إلى تعريف جرائم الحاسب الآلي (Computer) بأنها "هي كل عدوان بالارتكاب على أي قانون يتضمن في محتواه تقنية الحاسب الآلي (Computer) ويكون عرضة للتحقيق والاتهام"[٢] كان ذلك بالطبع بتأثير من اتجاهات المشرع الأمريكي في تعديل ١٩٩٦ لقانون البنية الوطنية للمعلومات The National Infrastructure Information Act (القسم ١٠٣٠)، الذي استوحي التجريم من الربط بين الحاسب الآلي (Computer) وتقنيته ككل، فتمخض هذا الاتجاه عن وجود ثلاثة أنواع من جرائم الذكاء الاصطناعي (A.I) التي يمكن ارتكابها عبر الحاسب الآلي (Computer) وذلك وفقاً للمنهج الأمريكي ، وهي [٣] :

النوع الأول : الجرائم التي يكون الحاسب الآلي (Computer) هدفاً لها، وهي نوعية من الجرائم يكون هدف المجرم فيها التوصل إلى سرقة بيانات من الحاسب الآلي (Computer) أو إحداث أضرار به أو بنظام تشغيله أو بالشبكة التي يعمل خلالها.

---

(1) Megel .A. Cardona, Artificial Intelligence and Education future, Op, Cit, P.20

(2) (SCALION) Robert – crime on the internet, fall 1996, p. 1. "compuer crime is any violation of the law that involve a knowledge of computer technology for their perpetration, investigation, or prosecution" available online in feb. 2000 at :
http://wings.buffallo.edu/complaw/complawpapers/scalion.html
- THOUMYRE - abuses in the cyberspace, op cit. P. 7

(٣) ويلاحظ أن هذا التقسيم كان قد وضعه الأستاذ الدكتور جميل عبد الباقي في مؤلفه – الجرائم الناشئة عن الحاسب الآلي – تقرير مقدم إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي – دار النهضة العربية القاهرة ١٩٩٢

النوع الثاني: الجرائم التي يكون الحاسب الآلي (Computer) وسيلة لارتكابها، وهذه النوعية من الجرائم تحدث عندما يستخدم المجرم الحاسب الآلي (Computer) لتسهيل ارتكاب بعض الجرائم التقليدية مثل الاحتيال على البنوك كما لو قام موظف بأحد البنوك باستخدام برمجية تحويل العملة لصالحه فيودع مبالغ محولة لحسابه عوضاً عن وضعها في مسارها الصحيح، وكذلك القيام بإعداد Produce أو نقل Transfer أو حيازة Possess آلة Device بما في ذلك الحاسب الآلي (Computer) بنية استخدامها في تزوير وثائق إثبات شخصية To (Falsify Identification documentation (18 USCode Sec. 1028

ولقد توسعت بعض التشريعات في مدلول مصطلح "أدوات التزوير Forgery Devices" لكي تشمل الحاسب الآلي (Computer) وملحقاته Equipment وبرمجياته Software إذا أعدت خصيصاً بغرض التزوير مثل قانون ولاية نيوجيرسي (N.J.Stat.ANN. Sec. C : 21-1) ،

النوع الثالث: الجرائم التي يكون فيها الحاسب الآلي (Computer) أداة لحفظ الأدلة دون أن يكون وسيطاً في الحصول عليها، كما هو الحال في قيام مروجي المخدرات والاتجار غير المشروع فيها، وكذلك معدي البرمجيات المعتدى على حقوق الملكية فيها وكذلك السرقة الإلكترونية التي تتم عدواناً على حقوق المؤلف بوضع سرقاتهم وملفاتهم وسجلاتهم في الحاسب الآلي (Computer).

ومما تجدر الإشارة إليه أن مثل هذا التقسيم السالف ليس جامعاً مانعاً للتعبير عن جرائم الذكاء الاصطناعي (A.I) ، إذ هناك من الجرائم التي ترتكب بواسطة الحاسب الآلي (Computer) ومع ذلك لا يمكن إدراجها في أي من الأقسام أو الأشكال الثلاثة مثلما هو الحال في جريمة سرقة وقت الحاسب الآلي (Computer) مثلاً[١] وهي جريمة يعرفها القسم Tit. 18 USCode Sec. 641

(١) د. جميل الصغير - الجرائم الناشئة عن استخدام الحاسب الآلي، القاهرة، دار النهضة العربية، ص ٢٤

من التقنين الأمريكي كجريمة من جرائم المعلوماتية[١]. وربما يكون السبب في التوسع السالف عائداً إلى أن إمكانيات الحاسب الآلي (Computer) لم تبرز إلى الوجود بالشكل الذي يجب أن تكون عليه، فكل ما نعلمه عن قدرات الحاسب الآلي (Computer) يقل كثيراً عما نعلمه عن قدرات الإنترنت (Internet). فهذه الأخيرة، وإن كانت لم تأخذ حظها كما ينبغي، فقد تناولها الساسة وفقهاء القانون والاقتصاد على المستوي الإقليمي والدولي بكثير من الامل وهي بعد في بداياتها، في حين إن مسيرة الحاسب الآلي (Computer) تبدو هادئة أو طبيعية. ومثل هذا الأمر وجد له تأثير كبير في الاتفاقية الأوروبية للجريمة عبر العالم الافتراضي المؤرخة ٢٠٠١/١١/٢٣ حيث اعترفت الاتفاقية، في المادة الأولى منها، بمصطلح "نظام الحاسب الآلي (Computer) Computer System" ولم تأخذ في الاعتبار مجرد مصطلح "الحاسب الآلي (Computer) Computer" فقد حددت الاتفاقية هذا المصطلح بكونه يشمل "أية آلة أو مجموعة مرتبطة فيما بينها أو ذات علاقة من الآلات، يمكن بإضافة برمجية إلى واحد أو أكثر منها، أن تقوم بمعالجة آلية للبيانات"[٢].

---

(1) United States v Sampsonm, 6 COMP, L. SERV. REP. 879 (N.D. Cal. 1978)

ففي هذه القضية فقد اعتبرت المحكمة أن الاستخدام غير المصرح به لحاسوب في مؤسسة حكومية يشكل جريمة عدوان على أملاك الحكومة Unauthorized use of computer time وفق ما هو مقرر في القسم Sec. 641 المشار إليه – انظر كذلك فيما يتعلق بالقسم ٦٤١ المذكور :

18 U.S.C. & 641. See : United States v. Friedman. 445 F. 2d 1076, 1087 (9th Cir.) (Theft of grand jury transcripts and information contained therein was theft of government property). Cert. denied. 404 U.S. 958 (1971) : United States v. Morison, 604 F. Supp. 655, 663-65 (D. Md. 1985) ("theft" of classified information supports embezzlement conviction); United States v. DiGillo, 538 F. 2d 972 (3d Cir). Cert. denied. 429 U.S. 871 (1971) (theft by photocopying government secords sufficient to support & 641 convocation) : United States v. MeAusland, 979 F.2d 970 (4th Cir. 1992) (theft of competitior's confidential bid information violates & 641).

(2) Art. 1 Definitions : "For purposes of this convention : Computer System means any device or a group of inter – connected or related devices, one or

لذلك يتجه بعض القانونيين إلى إحداث فصل في هذا الإطار من حيث تعريف جرائم الذكاء الاصطناعي (A.I) تعريفاً منفصلاً عن جرائم الحاسب الآلي (Computer)، بوصفها جرائم ناجمة عن استخدام الإنترنت (Internet)، وهو التعريف المبني على فهم عميق لطبيعة المشكلة من حيث ضرورة الفصل بين نوعي هذه الجرائم. حيث إن الإنترنت (Internet) أفاءت على القانون بأشكال إجرامية جديدة لم تكن معروفة، حتى في ظل التجريم عبر الحاسب الآلي (Computer) حيث إنه كنتيجة لظهور الإنترنت (Internet) أضحت المشكلة ليست فقط إحداثيات التمييز في إطار التجريم عبر الحاسب الآلي (Computer)، في محاولة تتعدى منطق التبسيط إلى التعقيد (مثال جرائم الذكاء الاصطناعي (A.I) – الجرائم المرتبطة بالحاسب الآلي (Computer) وتفصيلاتها أيضاً ...إلخ) [1]. ولعل ما انتهي إليه التطور الذي نراه سلبياً في توصيات مؤتمر G8 (الثمانية الكبار) عام ١٩٩٨ ليدعو إلى مزيد من التأمل في هذا الشأن، إذ تم التوصل إلى مصطلح High-Tech Crime أو جرائم التقنية العالية أو المتقدمة كنوع من محاولة التوسع في جرائم الحاسب الآلي (Computer) لكي تشمل كافة الجرائم التي يكون الحاسب الآلي (Computer) طرفاً فيها. وهذا كله يجعلنا نقرر أن هناك مفارقة مصطنعة بين جرائم الحاسب الآلي (Computer) وجرائم الإنترنت (Internet)، على الرغم من الالتصاق الذي يكاد يكون طبيعياً بينهما.

---

more of which, pursuant to a program, performs automatic processing of data"

(1) (KASPERSEN) Prof. Dr. Henrik W. K. – crimes related to the computer network. Threats and opportunities criminological perspective, p. 258. five issues in European criminal justice: corruption, women in the criminal justice system, criminal policy indicators, community crime prevention, and computer crime proccedings of the vi European colloquium on crime and criminal policy Helsinki 10-12 December 1998, European institute or crime prevention and control, affiliated with the united nations (heuni) p. O. Box 161, fin- 00131 Helsinki Finland publication series no. 34

- Thoumyre – abuses in the cyberspace, op. cit., p. 10

وهذا الاتجاه الذي نأخذ به يجد له أساساً فقهياً يسعي إلى إقامة بنيانه على النحو الذي يحقق مصلحة الإنسان قبل الآلة، إذ يذهب هذا الاتجاه إلى أن جرائم الإنترنت (Internet) هي "كل فعل أو امتناع عمدي ينشأ عن الاستخدام غير المشرع لتقنية المعلومات ويهدف إلى الاعتداء على الأموال المادية والمعنوية[١]. وعلى الرغم من التوجه الصحيح في تعريف جرائم الذكاء الاصطناعي على النحو السالف، سيما هو يوضح لزوم العمد، فكان هذا الرأي سباقاً عن اتجاهات الاتفاقية الأوروبية للجريمة عبر العالم الافتراضي المؤرخة ٢٠٠١/١١/٢٣، فإن هذا التعريف لا يخلو من نقد، حيث يستلزم الامتناع كنشاط مادي في مثل هذه الجرائم، وهو الأمر الذي لا يمكن تصوره في هذا الشأن.

ثالثا: ماهية جرائم الذكاء الاصطناعي (A.I)

يمكن وضع تعريف لجرائم الذكاء الاصطناعي إذا أخذنا في الاعتبار ثلاث نقاط رئيسة، وعلى ضوئها يمكن وضع تعريف متكامل يفيد في تحديد الجرائم الناشئة عن الإنترنت (Internet).

النقطة الأولي : موضوع العالم الافتراضي Cyberspace (وبالفرنسية Cyberespace) الذي هو عبارة عن العالم المرئي The virtual world أو المجال الحيوي للبيانات وحركتها المعلوماتية، وهو العالم المختفي في الآلة التقنية[٢]. والذي يطلق عليه الفقه العربي تسمية الفضاء الإلكتروني[٣]. وهو العالم الذي ابتكر فكرته كاتب الخيال العلمي الشهير William Gibson في روايته الشهيرة The NeuRomancer، التي أصدرها عام ١٩٨٤، حيث وصف في هذا الكتاب فانتازيا إلكترونية Fantasy Electronic[٤] تقابل فيها مجموعة هكر من مهرة الحاسب

---

(١) د. محمد سامي الشوا، ثورة المعلومات وإنعكاساتها على قانون العقوبات، ص ٧ .

(2) RCMP, op-cit.

(٣) د. جميل عبد الباقي الصغير، الأحكام الموضوعية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة ١٩٩٩، ص ٥ .

(4) (NICHOLSON) Keith – International Computer Crime : A Global Village Under Siege – New England International & Comparative Law Annual 1996 – New England School of Law P. I. available online is Sep. 2001 at : http://www.nest.edu/annual/vol2/computer.htm

الآلي (Computer)، وطالما نشاطهم الاختراق والعديد من المظاهر التي تكاد تصل في بعض الأحيان إلى منطق الجريمة عبر الإنترنت (Internet) كما هي مقررة في التشريعات المعاصرة.

وإذا كان قانون العالم الافتراضي / الإنترنت (Cyber Law) (Internet)، لا يشكل عقبة في إطار بناء نظريته – إن أمكن تكثيف الجهود نظرياً على الأقل – فإن الحال غير ذلك فيما يتعلق بتطبيق هذه النظرية وتنفيذها سيما في النطاق القضائي. ذلك إن تركيبة قانون العالم الافتراضي/ الإنترنت (Internet) ذات طبيعة مختلفة في الحقيقة عن تركيبة أي قانون آخر، فهو يتركب من طبيعة افتراضية ذات بعد دولي[1] يتطابق شكلياً مع مفاهيم العولمة، وليس مع المفاهيم التي يعرفها القانون الدولي، في الوقت الذي يتسع مدلوله ليشمل فروع القانون الأخرى. ذلك إنه من خلال مصطلح CyberLawهرع الفقه المقارن ليضع تفريعات جدية لهذا المصطلح تعمل في إطاره ووفق فروع القانون المعمول بها، مثل Cyberbehavior للدلالة على سلوكيات القانون المدني، ومصطلح CyberCrime للدلالة على سلوكيات القانون الجنائي، ومصطلح Cybercommerce للدلالة على سلوكيات القانون التجاري، ومصطلح Cyberinvestigation للدلالة على الإجراءات الجنائية في إطار الإنترنت (Internet)، ومصطلح Cybertribunal على المحاكمات عبر الإنترنت (Internet) ... إلخ.

إن عملية إحداث ملاءمة بين النظام القانوني القائم وبين الإنترنت (Internet) كانت قد برزت بداية حال موافقة الفقه النسبية على إمكانية التعامل القانوني مع الإنترنت (Internet) بأسلوب التنظيم النفسي للإنترنت Self – regulation ، بحيث يجب ألا يكون هذا التنظيم هو الأداة الوحيدة وإنما يقبل إلى جوار التنظيم القانوني بالأداة التشريعية تواجد أدوات تنظيمية نابعة من طبيعة الإنترنت

(1)TRANSNAIONAL NATURE OF CYBERSPACE, (CYBERCRIME AND CYBERPUNISHMENT< ARCHAIC LAW THERATEN GLOBAL INFORMATION p. 2 report prepared by : McConnell INTERNATIONAL http://www.mcconnellinternational.com with support from WITSA http://www.witsa.com December 2000 availale online in dec. 2000, at : http://www.mcconnellinternational.com/services/cybercrime.html

(Internet)، أي التقنية المعلوماتية. وسببية رفض وحدة التنظيم الذاتي كنظام قانوني للإنترنت يكمن في أن التنظيم الذاتي ليس مقنعاً بالدرجة الكافية[١] بما يجعل العالم الافتراضي آمناً بالدرجة الكافية التي تسمح بالأمن والاستقرار [٢]. على أن الأمر ليس على ذلك القدر من السهولة إذا تأملنا الاتجاه المضاد الذي يأخذ بضرورة التدخل القانوني لتنظيم العالم الافتراضي حيث إنه توجد لديه صعوبات أيضاً، من حيث إن أهم صعوبة تتمثل في تحديد طبيعة النظام القانوني الذي يحكم الإنترنت (Internet)، وهل تكفي النظم الأساسية في الدولة لحسم هذه الصعوبات وتذليل محتواها، أم إن العالم الافتراضي قام هكذا فجأة وبالتالي يمكن أن يوجد له أساس في النظم القانونية المعاصرة، إلا أن العقل القانوني لم يستظهر هذا الأساس بعد، وهنا فإن المسألة فقط تحتاج إلى مزيد من الوقت والتأمل والحكمة القانونية.

النقطة الثانية: ترتبط بالنتائج المترتبة في النظام القانوني حين فصل جرائم الحاسب الآلي (Computer Crimes Computer) عن جرائم الإنترنت (Internet) CyberCrime ، ومدى إمكانية قيام هذا الفصل تقنياً. والحقيقة أنه من الصعوبة بمكان فصل جرائم الحاسب الآلي (Computer) عن جرائم الإنترنت (Internet)، نتيجة لارتباط الإنترنت (Internet) بالحاسب الآلي (Computer) ارتباطاً تقنياً. إلا أن هذه الصعوبة سوف تتقلص كثيراً إذا أدركنا أن تقنية الحاسب الآلي (Computer) أعم كثيراً من تقنية الإنترنت (Internet). فهو – أي الحاسب الآلي (Computer)- ثورة حقيقية ذات أبعاد اجتماعية وسياسية واقتصادية وقانونية ليس لها نهاية، إذ كما أنتجت تقنية الحاسب الآلي (Computer) الإنترنت (Internet) فإن ذلك لا يعني نهاية المطاف في هذا الشأن، فالمؤشرات السائدة تشير إلى أن تقنيات جديدة للحاسب تبرز في الأفق قريبا ، وتدليلا على ذلك فإن دولا مثل كندا تربط جرائم الإنترنت (Internet) بجرائم الاتصال عن بعد Telecommunication Crime التي يمكن أن تقع بواسطة الإنترنت (Internet)

(1) RCMP, op-cit.
(2) CyberCrime And Cyberpunishment , archaic law threatens global information op-cit p. 2

كما يمكن أن تقع بواسطة الهاتف وجهاز الموجات الصغيرة Microwave والأقمار الصناعية Satellite وغير ذلك [١]

لذلك فإن الأرجح هو الاتجاه إلى التوسع في تعريف جرائم الذكاء الاصطناعي ومكمن التعريف الموسع هو السعي إلى بحث استقلالية لجرائم الإنترنت (Internet) تتنافى مع ربطها بالحاسب الآلي (Computer) وجرائمه . ولما كنا فيما سبق قد عرفنا الإنترنت (Internet) هي في الحقيقة الجرائم الناشئة عن استعمال هذا التواصل بين الشبكات وهذا اتجاه المشرع الأوروبي في اتفاقية الجريمة عبر العالم الافتراضي المؤرخة ٢٠٠١/١١/٢٣ وكذلك اتجاه المشرع الأمريكى حين رصده لمصطلح Protected Computer ولما كان التقسيم الأمثل لهذه الشبكة إلى ثلاثة أقسام كما عرضنا لذلك فيما سلف (شبكة المعلومات الدولية – البريد الإلكترونى- الاتصال المباشر)، فإن العدوان باستخدام الإنترنت (Internet) من خلال أقسامها هو الوضع الصحيح الذي يجب أن يكون عليه التجريم هنا لذلك نجد أن جرائم الإنترنت (Internet) في حقيقتها هي تلك الجرائم التي ترتكب بدواسة التواصل بين الشبكات .

ومن هذا المنطلق فإن الروية المحددة للانترنت لا تنطلق من الفكر النظري وإنما من الواقع العملي ، وهذا يستدعى البحث في مدى إمكانية المجتمع للتقبل الفكري لها ، فهي مجال حيوي Atmosphere في المجتمع قابل لربط عقليته Mentality بها ففي بعض الدول التي مرت بتجارب واقعة عن الإنترنت (Internet) أمكن لها أن تحدث تفاعلا إيجابيا يتواصل مع قانون الإنترنت (Internet) مثلما حدث في الفلبين على إثر قيام أحد طلبة الجامعة هناك بابتكار فيروس الحب I love You قامت الدولة بتكثيف جهودها لسن قانون في هذا الشأن سيما بعد التدخل الدولي نتيجة لكون الضرر عبر الحدود الدولية إلى نطاق عالمي فأصاب أجهزة حاسوب حول العالم .[٢] فالعالم الفعلي هو جزء من عالمنا غير

(1) FGSSC – available online in feb 2000 at :
http://www.usdoj.gov/criminal/cybercrime/search docs/toc.htm
(2) Cyber crime And cyberpubishment , archaic law threatens global information op – Cit P.4

منفصل عنه ، لذلك فهو ليس بعيدا عن إمكانية إحداث تنظيم قانوني له [١] ، بل إن الفقه ينادي بكينونة عقلية منفردة للانترنت فعلى مبدؤها عالمية التفكير وإقليمية الحركة [٢]

(1) Rcmp op-cit " a computers and telecommunications explode into the next century prosecutors and agents have begun to confront new Kind's explode into the next century prosecutors and agents have begun to confront new Kind's of problems "

(2) Thoumyre – abuse in the cyberspace op-cit P.9 : Think Globally and Act locally

المبحث الثاني

تصنيف جرائم الذكاء الاصطناعي

تتعدد انماط الجريمة في مجال الذكاء الاصطناعي، والتي يمكن تصنيفها إلى عدد من المحاور والتي تشكل جميعا انتهاكا يستحق العقاب وذلك على النحو التالي:

أولا: الجرائم المرتبطة بإنتحال الشخصيات عبر الذكاء الاصطناعي (A.I)

من الممكن الاختراق أو انتحال الهوية إما مادياً أو إلكترونياً. فالاختراق المادي يسمح بالدخول في مناطق خاضعة للسيطرة عن طريق بوابات إلكترونية أو آلية. وأسلوب الاختراق الأكثر شيوعاً هو أن يقف شخص غير مسموح له بالدخول أمام البوابة المغلقة حاملاً بين ذراعية متعلقات خاصة بالحاسب الآلي كالشرائط المغنطة desbandes أو ينتظر حتى يتقدم شخص مسموح له بالدخول ويفتح له الباب فيدخل معه في نفس الوقت. لذا فإنه يمكن القول بأن التواجد في صالات الحاسبات الآلية هو أمر حتمي لارتكاب هذه الجرائم[١]. وينطوى الفعل غير المشروع هنا على اطلاع غير مسموح به على المعلومات المختزنة في نظم المعلومات وله صور عديدة.

١- سرقة القائمة وهي عملية مادية بحتة يكتفي فيها السارق بسحب القائمة من الطابعة.

٢- الإطلاع على المعلومات والمقصود بذلك مطالعة المعلومات التي تظهر على شاشة الحاسب الآلي.

٣- التصنت المجرد على المعلومات ويتم ذلك عن طريق استخدام مكبر للصوت[٢] والذي يلتقط المعلومات والبيانات.

---

(١) انظر :

D. Parker, op. cit., p. 44 et s.

(٢) قبل أن يقوم Hacker باقتحام شبكة الحاسب الآلي، يجب عليه استخدام تسهيلات اتصال لكي يرتبط بالشبكة وقد يكون تكاليف الاتصال القانوني مع نظام الكمبيوتر المستهدف معرفة الـ Hackers قد تكون مرتفعة للغاية وقد يكون من الممكن تعقبها. لذا يقوم الـ Hackers بتوظيف أساليب فنية لتجنب هاتين= =المشكلتين: يقوم الـ Hackers بتوظيف أساليب فينة يطلق عليها عادة الـ Phreaking ومن تطبيقاتها ما يلي :

ويقصد بانتحال الهوية lusurpation didentitie سرقة شخصية مستخدم آخر ويتطلب الوصل إلى الحاسب الآلي أو إلى الطرفيات معرفة دقيقة لمستعمل الجهاز.

١- الاتصال التليفوني بواسطة النغمة :

وهو أسلوب نقلي يمكن التلاعب من خلاله في شبكات الاتصالات عن طريق استعمال تردد النغمات، أن النغمات يمكن استعمالها لتنشيط وتفعيل رقم تليفون غير متصل بما يتيح القدرة لهذا الشخص لاستكمال هذه الخطوط غير المتصلة كما لو كانت خطوطه الخاصة، إنم الفوائد المترتبة على هذه التقنية تشمل تكلفة المكالمة التليفونية لتي تضاف إلى فاتورة التليفون غير المتصل، علاوة على منع حدود أو متابعة أو تقصي هذه المكالمة.

٢- تلاعب Pabx : وهو أسلوب تقني يمكن للشخص بموجبه أن يطلب رقم تليفون pabx (وهو صندوق تحويل معد يحتوي على عدد من خطوط التليفون المختلفة). ويتم من خلال توصيل مكالمتهم إلكترونياً لواحد من لخطوط في هذا الـ pabox ثم استعمال هذا الخط للأغراض الخاصة.

٣- الاتصال الخارجي بالكمبيوتر : وبموجب هذه الوسيلة يستطيع الشخص أن يتصل برقم تليفون معين يتيح لهم بدوره فرصة الوصول إلى نظام الكمبيوتر أو الوصول إلى مركز اتصالات يتيح لهم نفس المزايا الموضحة في الأسلوبين السابقين.

٤- Austpac : وهي شبكة اتصالات تشرف عليها هيئة المواصلات الرسمية التي تقدم وصلات معينة بين أنظمة الكمبيوتر، أن الفواتير الخاصة باستعمال هذا النظام تعتمد على استعمال شبكة التعرف على المستعملين Network User Identieication Cnut ويتكون هذا النظام عادة من سلسلة من ٩ أرقام وهي شبيهة من حيث المبدأ برقم الـ PIN.

٥- الغش في بطاقات الاعتماد : هذا الأسلوب التقنيي يتضمن اقتباس تفاصيل بطاقات الاعتماد الخاصة بأحد المشتركين الذي يقوم بدوره بطلب مكالمة تليفونية لصالح الطالب وقيد قيمة المكالمة على بطاقة الاعتماد.

٦- الاعتراض المادي : إن عملية الاعتراض المادي لخط تليفوني هي عملية بسيطة وتؤدي إلى نفس الفوائد مثل الاتصال بالنغمة.

٧- الوصلات غير القانونية : وهي عبارة عن تنشيط وتشغيل خدمة غير متصلة بدون علم شركة الاتصالات ثم استعمالها حسب رغبتك عن طريق تليفون عادي بدون أو تتلقي الفاتورة. وهذا النوع من الاعتراض يتميز بأنه دائم ومسمر.

انظر :

Franklinclrk, investigating computer crime, Ed. CRC page 50.

كما أن فحص الهوية يرتكز على مجموعة معلومات متوافقة يستخدمها المستعمل ككلمة السر[١] أو أي جملة خاصة بالمستعمل أو أي خاصية فسيولوجية كالبصمة الرقمية أو ملامح للوجه أو هندسة الكف أو الصوت بالإضافة إلى أي شيء يمتلكه المستعمل كالبطاقة الممغنطة أو المفتاح المعدني. فلو تمكن أي إنسان من الحصول على هذه المجموعة من المعلومات المتوافقة يصبح قادراً على انتحال شخصية المستعمل.

ثانيا: الجرائم ذات البعد المالي عبر الذكاء الاصطناعي (A.I)

يعني الائتمان Credit إضافة مستقبلة للأموال المشمولة بالحماية بحيث تضمن هذه الإضافة كل التصرفات المالية للشخص. والمبدأ الأساس في الائتمان هو الحماية، إذ برز الائتمان على أثر تصاعد حدة جرائم السرقة بالإكراه، والتي وصلت إلى أعلى معدلاتها في العدوان على الحياة في مقابل نهب المال من الضحايا. فالهدف يظل هو اختلاس الأموال إلا أن السارق فضلاً عن كونه يستخدم الإكراه فإنه كذلك يفضل ألا يترك أثراً وراءه يمكن أن يقود إليه. وعلى الرغم من كون قاعدة الحماية هي الأموال فإن الجريمة استطالت أيضًا الائتمان لكون الأموال عبر الائتمان تتحول إلى أرقام موضوعة على كروت يستلمها المؤتمن من المصرف الذي يتعامل معه.

---

(١) بعض كلمات السر يتم وضعها من خلال مدير النظام المعلوماتي والبعض الآخر يتم استخدامه من وحي المستخدمين أنفسهم. وبصرف النظر عن ذلك فإن كلمة السر يجب أن تكون مميزة لكل حساب ويجب تغيير وحذف الحسابات التي ليس لها كلمة سر وينصح بتجنب استعمال كلمات السر التي يسهل الوصول إليها مثل استعمال الأسماء الأولى والأخيرة وتاريخ الميلاد وأرقام الضمان الاجتماعي أو رقم رخصة القيادة فهذه الكلمات يمكن التنبؤ بها.
كما يعرف القراصنة كلما السر الأكثر شهرة والتي يميل الناس إلى اختيارها لذا يحظر استخدامها مثل كلمة سر passwred وكلمة ادخل Enter وافتح Open وكمبيوتر Computer ويحذر هذا الاستخدام كلمات السر المرتبطة بالهواية كما يحذر تجنب كلمات السر ذات المقطع الكبير أو تلك المتعلقة بمجموعة حروف أو أرقام.
راجع في ذلك :
E. Quarantiello (cybercrime) p. 94.

وبتطور التقنية في ظل ثورة الذكاء الاصطناعي (A.I) نشط الائتمان، سيما عبر التجارة الإلكترونية/ الإنترنت (Internet) على وجه التحديد. فالتعامل المالي عبر الإنترنت (Internet) كما أنه استطاع استيعاب فكرة ظهور أشكال جديدة للنقود، فإنه كذلك يستطيع استيعاب فكرة الائتمان، خاصة إذا علمنا أن التعامل بالائتمان عبر الإنترنت (Internet) له سوابق تاريخية. إذ يكفي أن تضع اسمك ورقم بطاقة الائتمان الخاصة بك لكي تصل إلى مبتغاك أو غرضك التجاري كالبيع والشراء والاشتراك في مؤسسات وأندية...الخ. ويمتد نشاط التعامل بهذه البطاقات إلى النواحي العالمية؛ إذ يجوز اختراق الحدود بمقتضى الائتمان[١] أو بالأحرى تقلص فكرة رقابة الدولة عليها[٢].

وقد كان التشريع الفرنسي من أوائل التشريعات التي قررت سلوك المسلك الجنائي حال العدوان الإجرامي على كروت الائتمان، وذلك منذ العام ١٩٨٨ بقانون Godfrain (نسبة إلى النائب الذي تقدم بمشروع القانون إلى الجمعية الوطنية) المؤرخ ١٩٨٨/١/٥، وهو القانون الذي أضيف إلى نص المادة (٥-٤٦٢ عقوبات فرنسي جديد) بشأن الاحتيال Faux على بطاقات الائتمان. ومما تجدر الإشارة إليه أن الاحتيال المذكور Faux قد تولى المشرع الفرنسي تفسيره على ضوء المادة (١-٤٤١- عقوبات فرنسي جديد). ويشار هنا إلى القانون المؤرخ ٣٠ سبتمبر ١٩٩١ المعدل للمرسوم المؤرخ ١٩٣٥/١٠/٣٠ بإصدار قانون الصك قد أضاف موادًا تتعلق ببطاقات الائتمان وذلك بالعقاب على تقليد Contrfacon وتزييف Falsification هذه البطاقات.

وتتخذ أشكال العدوان على الائتمان عبر الذكاء الاصطناعي (A.I) أحد شكلين:

(١) الاستيلاء على أرقام كروت الائتمان: إذ إن لكل كارت ائتمان عنوانًا فرديًا خاصًا ID number يتميز به عن غيره، تمنحه المؤسسة المالية

---

(١) د. حازم الببلاوي: النظام الاقتصادي الدولي المعاصر، عالم المعرفة، العدد ٢٥٧/الماء/ مايو ٢٠٠٠، الكويت، ص١٥٤.

(٢) المرجع السابق، ص١٦٥.

للمشترك لديها في هذه الخدمة بحيث تحل محل التعامل بالأموال السائلة.

ولقد امتد نشاط بطاقات الائتمان إلى الإنترنت (Internet) فانفتح المجال لها لكي تضع عملية استخدامها في محك على درجة عالية من الخطورة إزاء مظاهر الاحتيال التي يتم بها الاستيلاء على أرقام هذه البطاقات بشكل غير مشروع، وعلى النحو الذي يحقق تكامل جريمة الاستيلاء على كروت ائتمان.

وعلى الرغم من أن اتجاهًا فنيًا يذهب إلى أن الحيازة غير المشروعة لأرقام كروت الائتمان التي تتم عبر الإنترنت (Internet) إنما هي على درجة كبيرة من الصعوبة، كعملية تقنية تحتاج إلى برمجة معقدة، وبالتالي تعد حركة الحيازة المادية لها أسهل بكثير من حيازتها عبر الإنترنت (Internet) فإن حالات اختلاس هذه الأرقام عبر الإنترنت (Internet) من الخطورة بمكان وهو ما دفع المشرع الفيدرالي الأمريكي إلى عدها جريمة وفق 18 U.S.C. 1030(a)(1)(7) [(١)]. فقد حدث في عام ١٩٩٦ أن تم اختراق حاسوب محمول LAPTOP يحتوي على ٣١٤.٠٠٠ رقم لكروت ائتمان تخص أحد المكاتب التابعة لمؤسسة Visa Card INT في كاليفورنيا، وفي عام ١٩٩٧ قام Carlos Sadalgo Jr. (37 عامًا) باستخدام حاسوب في جامعة سان فرانسيسكو واختلس أسماء مالكي وأرقام log-ons عدد ١٠٠.٠٠٠ كارت ائتمان وكذلك بيانات أخرى من خلال اختراقه لمجموعة مزودي خدمات إنترنت ISPs وقام بوضعها على اسطوانة مضغوطة CD ثم قام بتشفيرها وعرضها للبيع بمبلغ مائتين وخمسين ألف دولار، ولقد اكتشف عملاء المباحث الفيدرالية هذه الجريمة وحوكم سادالوجو وعوقب بالسجن ثلاثين شهرًا [(٢)].

---

(١) انظر:

- Hughes, Carole (1999). The Relationship of Use of the Internet and Loneliness among College Students. Dissertation Abstract . Vol. 60 (3 – A).

(2) The CFAA makes it a crime for an unauthorized user to access a computer that is federally owned or is a « protected computer » for the purpose of 1) obtaining records from a bank, credit card issuer, or consumer reporting agency ; 2) committing fraud or extortion ; 3) transmitting destructive viruses or commands ; 4) trafficking in stolen passwords ; or 5) threatening to

(٢) العدوان على التوقيع الإلكتروني عبر الذكاء الاصطناعي (A.I):

التوقيع الإلكتروني كأحد مظاهر التوقيع عامة كان – ولا يزال – أحد اهتمامات المشرع المقارن، ومن ذلك المشرع الأوروبي الذي أصدر توجيهًا في عام ١٩٩٥ للشروع في تشكيل لجنة خبراء لكي تتولى وضع مشروع التوقيع الإلكتروني، وفي ١٦ الصيف/ يونيو ١٩٩٨ تقدمت اللجنة بمشروعها هذا مقترحة إصدار مجلس أوروبا توجيهًا بالخصوص، وفي ٢٢ الطير/ إبريل ١٩٩٩ وضع المشروع النهائي للتوجيه، ولقد قام البرلمان الأوروبي في ١٢ الكانون/ ديسمبر ١٩٩٩ بإعداد نصوص التوجيه المذكور ليخرج علينا في ثوبه الأخير. ولقد أصدر المشرع الألماني قانون الإنترنت (Internet) لسنة ١٩٩٧ يتضمن مجموعة نصوص حول الإنترنت (Internet) المؤرخ في ٢٢ يوليو ١٩٩٧ ومن بينها نصوص تتعلق بالتوقيع الإلكتروني.

كذلك اعترف المشرع الفرنسي بالتوقيع الإلكتروني حيث تنص المادة (٤-١٣١٦) من القانون المدني الفرنسي بعد تعديلها بالقانون رقم ٢٣٠-٢٠٠٠ المؤرخ ١٣ مارس ٢٠٠٠ حيث تقرر بأن التوقيع الإلكتروني يعد وسيلة تعامل معترفًا بها، ومفترضًا صحته Pésumée إلى حين إثبات العكس. ولقد صدر المرسوم التنفيذي لهذا التعديل رقم ٢٧٢-٢٠٠١ المؤرخ ٢٠٠١/٣/٣٠ بشأن تطبيق المادة (٤-١٣١٦) من القانون المدني الفرنسي المتعلقة بالتوقيع الإلكتروني، حيث تضمن في المادة (١/١) تعريفًا أكثر تحديدًا للتوقيع الإلكتروني بأنه "معطيات ناتجة عن استعمال طريقة ردًا على شروط معرفة في صدر الجملة المقررة في الفقرة الثانية من المادة (٦-١٣١٦- مدني)".

---

damage a computer system in order to extort money or other things of value. A « protected computer » is a computer 1) used exclusively by a financial institution or the United States Government ; 2) used on a nonexclusive basis but where the conduct affects use by the financial institution or the government ; or 3) used in interstate or foreign commerce or communication. This last element is intended to keep the federal government out of purely local computer crimes, but the multistate nature of Internet transmission suggests that almost any Internet activity will amount to « interstate commerce ». see : James Garrity & Eoghan Casey. Internet Missue in the Workplace : A Lawyer's Primer, op. cit., at 14.

وفي إطار النظام القانوني الإنجليزي استطاع القضاء الإنجليزي في قضية Goodman V. J. Eban. Ltd تحديد الأصالة Authentication بالإضافة إلى مناهج التوقيع الإلكتروني. على أن الأمر لم يقف عند هذا الحد وإنما قامت إدارة التجارة والصناعة الإنجليزية Department of Trade and Industry في مارس ١٩٩٩ بإصدار وثيقة استشارية Consultation Document بعنوان Building Confidence in Electronic Commerce تم هيكلتها على ضوء التوجيه الأوروبي المشار إليه أعلاه، وبناء على هذه الوثيقة أصدر البرلمان الإنجليزي قانون الاتصالات للمملكة المتحدة المؤرخ ٢٠٠٠/٥/٢٥ The UK Electronic Communications Act الذي ينص في القسم (٧) من على تعريف للتوقيع الإلكتروني[١]. وأما المشرع البلجيكي فقد أصدر القانون المؤرخ ٢٠ أكتوبر ٢٠٠٠ الذي أضاف إلى القانون المدني البلجيكي المادة (٢٢٨١) مقرراً الاعتراف بالتوقيع الإلكتروني إلى جوار اعترافه بالتوقيعات التي ترد عبر الفاكس والبريد الإلكتروني والبرقيات والتلكس وبأية وسيلة أخرى[٢].

أما المشرع الأمريكي فقد اهتم اهتمامًا كبيرًا بموضوع التوقيع الإلكتروني لكونه أداة فعالة في حركة المعاملات المدنية والتجارية، وتحديدًا كان للمشرع الولائي الأمريكي الأسبقية في هذا الإطار، حيث أصدر مشرع ولاية Utah في عام ١٩٩٥ أول تشريع للتوقيع الإلكتروني The digital signature act

---

(1) Section 7(1) provides: In any legal proceedings:
(a) an electronic signature incorporated into or logically associated with a particular electronic communication or particular electronic data, and
(b) the certification by any person of such a signature, shall each be admissible in evidence in relation to any question as to the authenticity of the communication or data or as to the integrity of the communication or data, See: Chris Reed-What is a signature?, op. cit., at 15.

(2) 20 OCTOBRE 2000, Loi introduisant l'utitisation de moyens de télécommunication et de la signature électronique dans la procédure judiciaire et extrajudiciaire.

والمادة (٢٢٨١- مدني بلجيكي) هي المادة التي كان المشرع البلجيكي قد ألغاها بمقتضى القانون المؤرخ ١٩٤٩/١٢/١٥. ولقد أعادها إلى الحياة في ثوب جديد بمقتضى القانون المؤرخ ٢٠٠٠

of 1995 الذي تم إلغاؤه وإعادة إصدار تشريع آخر في عام ١٩٩٦، وكان من بين الأغراض التي سعى مشرع ولاية يوتا الأمريكية بإصداره هذا التشريع هو التخفيف من حدة الاحتيال بالتزوير والنصب على التوقيعات ككل[(١)]. ثم تلا ذلك ولاية كاليفورنيا بقانون ٥ سبتمبر ١٩٩٥ الذي، بعد أن اعتبر التوقيع الإلكتروني في مرتبة التوقيع المادي، قام بتعريف التوقيع الإلكتروني في القسم (٥-١٦) من كود الحكومة الولائية The Government Code بأنه "تحديد إلكتروني للهوية تم إعداده بواسطة الحاسب الآلي (Computer) ومعتمد من قبل مستخدمه لكي يكون له ذات القوة والأثر للتوقيع المادي أو اليدوي ولكن لا يشمل هذا التعريف إمكانيات التشفير"[(٢)]. لتتوالى بعد ذلك مظاهر الاهتمام بالتوقيع الإلكتروني من قبل المشرع الولائي الأمريكي مثل تشريع ولاية أويامنغ Wvoming لعام ١٩٩٥، ثم تشريع ولاية واشنطن Washington الصادر في ٢ مارس ١٩٩٦ الذي اعتمد على تشريع ولاية يوتا، ومما تجدر الإشارة إليه أن تشريع واشنطن تقرر نفاذه مع الأول من شهر يناير ١٩٩٨.

ولكي يتم العدوان على التوقيع الإلكتروني فإن ذلك يأخذ شكل العدوان على الأساليب الآمنة التي يتولاها طرف ثالث محايد Neutral Third Party، هو مقدم خدمات الإنترنت (Internet) Online Service Provider OSPs، وذلك بالعدوان على وسائل التشفير الضرورية من مفتاح عام وآخر خاص. على أن الأمر قد يأخذ شكلاً آخر أكثر سهولة يتمثل في حالة تتبع التوقيع الإلكتروني لشخص ما، بما يستدعي الأمر هنا لزوم إحداث اختراق تام من خلال معرفة الخادم المشترك فيه هذا أو ذاك الشخص، ثم القيام بعد ذلك بالبحث فيه عن الهوية الإلكترونية IP الخاصة

(1) William E. Wyrough, JR & Ron Klein- The electronic signature act of 1996: Breaking down barriers to widespread electronic commerce in Florida, op. cit., at 429.

(2) « An electronic identifier, created by computer, intended by the party using it to have the same force and effect as the use of a manual this definition does not include encryption. Further, signature », id at 431.

بذلك الشخص، حتى يتوصل إليها ثم بعد ذلك القيام باستنساخ التوقيع الإلكتروني خاص به.

ثالثا: الجرائم ذات البعد الأخلاقي باستخدام الذكاء الاصطناعي (A.I)

يمكن أن يتسع الترويج عبر الذكاء الاصطناعي (A.I) كذلك ليشمل المحادثة الشفهية بأية وسيلة كانت كالتي تتم عبر الفيديو الرقمي أو البث الحي له بطريق الإنترنت (Internet) أو بطريق الدوائر المغلقة كعرض الشهادة في المحاكم أو تناول موضوعات عامة عن بعد. ولعل أخطر مظاهر الترويج السمعي المرئي هو أن يلحقه صفة الفضح فيما يصطلح عليه باللغة الإنجليزية بعبارة Cyber Audio – Visual Indecent، فمثلاً القيام بالاتصال بالغير باستخدام الإمكانيات السمعية المرئية عبر الإنترنت (Internet)، مع القيام بحركات أو إيماءات فاضحة، من الأمور التي يمكن أن تشكل جريمة ما هنا، ويزداد الأمر صعوبة حالة وجود نوع من التداول لمثل هذه الحركات السمعية المرئية الفاضحة، من خلال تسجيلها والقيام بتداولها عبر الإنترنت (Internet)، والمشرع المقارن يهتم في صيغة تقليدية بمثل هذه الجرائم، من خلال التعامل بالفيديو في العالم المادي كما هو الشأن فيما هو مقرر في المادة (١/١٧٨- عقوبات مصري) [١] التي امتدت إلى المعاقبة على حيازة شرائط فيديو مخلة بالآداب، سواء كانت هذه الحيازة بقصد الاتجار أو العرض بمقابل أو بدون مقابل[٢]. وهو الأمر المعاقب عليه

---

(١) تنص المادة (١/١٧٨- عقوبات مصري) على أنه "يعاقب بالحبس مدة لا تزيد على سنتين وبغرامة لا تقل عن خمسة آلاف جنيه ولا تزيد على عشرة آلاف جنيه أو بإحدى هاتين العقوبتين كل من صنع أو حاز بقصد الاتجار أو التوزيع أو الإيجار أو اللصق أو العرض مطبوعات أو مخطوطات أو رسومات أو إعلانات أو صورًا محفورة أو منقوشة أو رسومات يدوية أو فوتوغرافية أو إشارات رمزية أو غير ذلك من الأشياء أو الصور عامة إذا كانت منافية للآداب العامة.

(٢) طعن جنائي مصري رقم ٣١١٦ لسنة ٥٥ق جلسة ١٩٨٧/١٠/٢٨ المكتب الفني لمحكمة النقض المصرية السنة ٣٨ صفحة رقم ٨٧٨- ولقد أشارت المادة (٢/١) من قانون المطبوعات المصري رقم ٢٠ لسنة ١٩٣٦ (الوقائع المصرية العدد ٢٣ في ١٩٣٦/٣/٢- موسوعات التشريعات العربية) إلى أنه يقصد بالتداول بين المطبوعات أو عرضها لبيع أو توزيعها أو إلصاقها بالجدران أو

في القانون الأمريكي بمقتضى القسم (18 US Code Sec 2252) التي تعاقب على الاتجار والنقل Transporting والحيازة Possession لبرمجيات حاسوب تتضمن دعارة أطفال[١].

ونتيجة لمبادرة البيت الأبيض المذكورة فإنه في عام ١٩٩٨ أصدر الكونجرس الأمريكي القانون رقم Public Law 105-314 بشأن حماية الأطفال من التعدي الجنسي[٢]. ولقد تضمن هذا القانون حث النائب العام الأمريكي على التعاون مع الأكاديمية الوطنية للعلوم/ مجلس البحوث الوطنية فيها، على إعداد دراسة متكاملة لبحث مدى إمكانية تفعيل القانون الجنائي في القضايا الأخلاقية، والتي أنتجها التعامل السلبي مع تقنية المعلومات/ الإنترنت (Internet). على أن يتم وضع هذا التقرير في خلال سنتين من تاريخ صدور القانون المذكور. ولقد تم وضع التقرير في العام ٢٠٠٠ متضمنًا الخطوات الفعالة من الوجهة العلمية من قبل الأستاذين Herb Lin, PhD, Michele Kipke, PhD، بالتعاون مع جهات أخرى ذات علاقة. ولقد وجد التقرير أن مشكلة الدعارة المصورة Pornography ذات أساس من ناحيتين، الأولى كونها تعد داخلة في نطاق اهتمام قسم اجتماعي له دور في المجتمع، حتى وإن كان سلبيًا. أما الناحية الثانية فيتعلق بالتحديد القضائي لمصطلح الدعارة الذي يتخذ مفهوما يتسع ليشمل الطابع المتغير فيها vary widely من نطاق اجتماعي إلى آخر Vary by community[٣].

عرضها في شبابيك المحلات أو أي عمل آخر يجعلها بوجه من الوجود في متناول عدد من الأشخاص. انظر: د. جميل الصغير، الأحكام الموضوعية، السابق، ص٨٩.

(1) USA v.Miller, App 11th Cir No.98-8228, Feb. 4-1999, Available online in March 1999 at:
http://www.lp.findlaw.com/scripts/getcase.pl?navby=search&case.../988228man.htm

(2) Protection of children from Sexual predators act of 1998 Title 9 section 901. US Code. Id at 422.

(3) Herb Lin, PhD hlin@nas.edu, Michele Kipke, PhD mkipke@nas.edu – Tools and Strategies for Protecting Kids from Pornography and Their Applicability to other Inappropriate Internet Content, P.4.

كذلك يجرم القانون الأمريكي تشغيل Employ القصر Minors أو دفعهم Induce إلى المشاركة في صور متحركة Visual depiction تتضمن حركة جنسية مباشرة، إذا كان التصوير قد تم باستخدام حاسوب عبر مؤسسات تجارية في الولايات أو في خارج الولايات المتحدة (18 US Code Sec. 2251). كذلك يحظر القانون الأمريكي استخدام الحاسب الآلي (Computer) لبيع Sell أو نقل Transfer حق الوصايا على قاصر مع العلم بأن هذا القاصر سوف يتم استخدامه لإعداد صور متحركة تتضمن سلوكًا جنسيًا مباشرًا ((A) 18 US Code Sec. 2251). كما يجرم القانون الأمريكي استخدام الحاسب الآلي (Computer) لنقل Transport دعارة الأطفال Child pornography عبر الولايات أو عبر مؤسسات تجارية أجنبية (18 US Code Sec. 2252 & 2252 (A)) [١].

أما في فرنسا فإن المادة (٢٤-٢٢٧) من قانون العقوبات الفرنسي الجديد تعد حجر الأساس في إطار دعارة الأطفال[٢]. حيث يعاقب معد مواقع دعارة الأطفال وفقًا للمادة (٢٤-٢٢٧) في فقرتها الأولى من ذات القانون، أما الفقرة الثانية منها فتعاقب مستخدم الموقع. وأما قانون العقوبات البلجيكي فقد تضمن في المادة (383 bis) منه (المضافة بالقانون المؤرخ ١٩٩٥/٤/١٣) [٣] العقاب على عرض Expose وبيع Vendu وتأجير Loue وتوزيع Distribute أو دعم موقع

---

(1) USA v. Hay, App. 9th Cir. No. 99-30101, 24 Oct. 2000, Available online in Oct. 2000 at: http://laws.findlaw.com/9th/9930101.html.

(2) Guillam Desgens – Pasanau, Au Centre des debat actuels: La protection des mineurs sur l'internet -24/7/2001. disponible enligne en Juillet 2001 a: http://www.droit-technologie.org/1.2.asp?actuid=1604298204.

انظر القانون رقم ٩٨-٤٦٨ المؤرخ ١٩٩٨/٦/١٧ بأن منع والمعاقبة على الجرائم وحماية القصر- تعاقب كل من يقوم ببث مواقع دعارة أطفال.

(3) Sur le plan penal, deux infractions contenues dans le Nouveau Code Penal (NCP), ayant pour finalite la protection des mineurs, meritent, concernant le reseau Internet, une attention particuliere. Ainsi: - "le fait, en vue de sa diffusion, de fixer, d'enregistrer ou de transmettre l'image d'un mineur lorsque cette image presente un caractre pornographique".

مـرئي Remi des supports Visuals لأوضـاع جنسـية ذات طـابع فـاحش Pornographique، وذلك باستخدام قصر ممن لم يبلغوا السادسة عشرة مـن عمرهم، ويعاقب كذلك معد مثل هذه المواقع وكذلك مستوردها[1].

(1) Thibault Verbiest – Pornographique e Internet: comment reprimer? 19 Mai 2001, disponible enligne en juin 2001 a: http://www.droit-technologie.org/1.2.asp?actu.id=2099182987.

المبحث الثالث

المعوقات المرتبطة بالضبط التشريعي لجرائم الذكاء الاصطناعي (A.I)

إن أهم ما يميز جرائم الذكاء الاصطناعي (A.I) صعوبة اكتشافها وإثباتها [١].
علاوة على ما تتميز به إجراءات جمع الأدلة فى هذا المجال من ذاتية خاصة.

أولا:معوقات إثبات جرائم الذكاء الاصطناعي (A.I)

تتسم الجرائم التى تقع على الحاسبات وشبكات المعلومات بأنها غير مرئية فى العديد من حالاتها[٢]. حيث لا يلاحظها المجنى عليه غالبا أو يدرك وقوعها . وإخفاء السلوك المكون لها وطمس أو تغطية نتائجها عن طريق التلاعب غير المرئى فى النبضات أو الذبذبات الالكترونية التى تسجل البيانات عن طريقها ليس مستحيلا فى الكثير من أحوالها بحكم توافر المعرفة والخبرة الفنية فى مجال

---

(١) انظر في ذلك :
د. محمد زكي – الإثبات في المواد الجنائية ، ص١٦ ، د.محمد محي الدين عوض ، مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات ، ص٣٩٨ – ٣٩٩ د. هدى حامد قشقوش ، جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات ، بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي ، القاهرة ٢٥-٢٨ أكتوبر ١٩٩٣ ، منشورات دار النهضة العربية ١٩٩٣ ، ص٤٥٠ و٤٧٦ و٥٧٦. د. زكي أمين حسونة ،جرائم الكمبيوتر والجرائم الأخرى في مجال التكتيك المعلوماتي – بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي القاهرة، ٢٥-٢٨ أكتوبر ١٩٩٣ ، العقيد علاء الدين محمد شحاته – رؤية أمنية للجرائم الناشئة عن استخدام الحاسب الآلي – بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي – القاهرة ٢٥-٢٨ أكتوبر ١٩٩٣.

(٢) إذ تقع هذه النوعية من الجرائم في بيئة لا تعتمد التعاملات فيها أصلا على الوثائق والمستندات المكتوبة بل على نبضات اليكترونية غير مرئية لا يمكن قراءتها إلا بواسطة الحاسب الآلي والبيانات التي يمكن استخدامها أدلة ضد الفاعل يمكن في أقل من الثانية العبث به أو محوها بالكامل لذا فإن للمصادفة وسوء الحظ دورا في اكتشافها يفوق دور اساليب التدقيق والرقابة ومعظم مرتكبيها اللذين تم ضبطهم وفقا لما لاحظه أحد الخبراء، إما أنهم قد تصروفوا بغباء أو أنهم لم يستخدموا الأنظمة المعلوماتية بمهارة : انظر :
John Eaton and Jermy smithers, this is it. Amangagrs Guide to information technology , London, Philip Allan , 1982p.263
مشار إليه د. هشام محمد فريد رستم، بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنت في الفترة من ١-٣ مايو ٢٠٠٠ بجامعة الإمارات العربية المتحدة بعنوان الجرائم المعلوماتية).

الحاسبات لدى مرتكبها.[١]. اختلاس المال عن طريق التلاعب فى برامج الحاسب ومحتوياته، وغالبا ما يتم فى مخرجات الحاسب تغطيته وستره. والتجسس على ملف البيانات كان خطأ مصدره البرامج أو الأجهزة أو نظام التشغيل أو التصميم الكلى للنظام المعلوماتى. ونتيجة لهذه الصعوبة أصبح لإمكانية إخفاء جريمة الذكاء الاصطناعي (A.I) عن طريق التلاعب فى البيانات مصطلحا يستخدم فى أبحاث علم الإجرام الأمريكية وهو (الطبيعة غير الأولية لمخرجات الحاسب المطبوعة) .Second-hand Nature computer printouts

ثانيا: معوقات أدلة جريمة الذكاء الاصطناعي (A.I)

تتمثل أهم المعوقات المرتبطة بأدلة جرائم الذكاء الاصطناعي (A.I) كما يلي:

(أ) انعدام الدليل المرئى

يلاحظ أن ما ينتج عن نظم المعلومات من أدلة عن الجرائم التى تقع عليها أو بواسطتها ما هى إلا بيانات غير مرئية لا تفصح عن شخصية معينة وهذه البيانات مسجلة الكترونيا بكثافة بالغة وبصورة مرمزة[٢]. غالبا على دعائم أو وسائط للتخزين ضوئية كانت أو ممغنطة لا يمكن للإنسان قراءتها وإن كانت قابلة للقراءة من قبل الآلة نفسها ولا يترك التعديل أو التلاعب فيها أى أثر مما يقطع أى صلة بين المجرم وجريمته ويعوق أو يحول دون كشف شخصيته[٣].وكشف وتجميع أدلة بهذا الشكل لإثبات وقوع الجريمة والتعرف على مرتكبيها هو أحد أبرز المشاكل التى يمكن أن تواجه جهات التحرى والملاحقة. وتبدو هذه المشكلة بشكل عام فى سائر مجالات التخزين والمعالجة الآلية للبيانات حيث تنتفى غالبا قدرة ممثلى الجهات المختصة على أن يتولوا بطريقة مباشرة فحص واختبار البيانات المشتبه فيها وتزداد

---

(١) انظر في ذلك :

Jay , J. Becker the Trial of computer crime (1980), 2 computer Law , Journal 441

مشار إليه الدكتور هشام محمد فريد رستم ، سابق الإشارة إليه.

(2) Les dificultes techniques sont liees aux methoded de cryptologie employees sur le reseua .

La criminamite informatique sur linternet , p. 58

(٣) انظر في ذلك :

Ulrich , sieber, ibid, p. 140

جسامة هذه المشكلة بوجه خاص فى حالة التلاعب فى برامج الحاسب نظرا لتطلب الفحص الكامل للبرنامج واكتشاف التعليمات غير المشروعة المخفية داخله قدرا كبيرا من الوقت والعمل[١].

(ب) سهولة محو الدليل أو تدميره فى فترة زمنية يسيرة

من الصعوبات التى يمكن أن تعترض عملية الإثبات فى مجال جرائم الذكاء الاصطناعي (A.I) سهولة محو الجانى أو تدميره لأدلة الإدانة فى فترة زمنية وجيزة فضلا عن سهولة تنصله من هذا العمل بإرجاعه إلى خطأ فى نظام الحاسب أو الشبكة أو فى الأجهزة ومن الأمثلة الواقعية قيام أحد مهربى الأسلحة بإدخال تعديلات على الأوامر العادية لنظام تشغيل حاسب صغير يستخدمه فى تخزين عناوين عملائه والمتعاملين معه بحيث يترتب على إدخال أمر إلى الحاسب من خلال لوحة مفاتيحه بالنسخ أو الطبع أو تدمير البيانات كلها. ومع أن تعديل برمجة نظام تشغيل الحاسب كان قد أجرى خصيصا بواسطة الفاعل للحيلولة دون نجاح أجهزة الملاحقة فى إجراءات المتوقعة للبحث عن الأدلة وضبطها إلا أنه لم يفلح فى تحقيق هذا الهدف نتيجة لتوقع المتخصصين لمعالجة البيانات بالجهاز المركزى

---

(١) وتدليلا على تأثير غياب الدليل المرئي في إعاقة اجراءات الضبط وملاحقة مرتكبي الجرائم التي تقع في مجال تكنولوجيا المعلومات يشير الأستاذ sieber إلى حالة واقعية شهدتها المانيا الاتحادية سابقا عام ١٩٧١ تلخص وقائعها في اكتشاف شركة طلبياتها بريدية mail order firm سرقة أشرطة ممغنطة تخصها تحتوي ٣٠٠٠٠٠ عنوانا لعملاتها وتمكنها من استصدار أمر من المحكمة . معروف باسم وقف الأعمال injuction باستعادة كل العناوين من شركة منافسة كانت قد حصلت على هذه العناوين من مرتكبي السرقة ، وتنفيذا لهذاالأمر سمحت الشركة المنافسة لمساعدة مأمور التنفيذ بدخول مقرها ومركز الحاسب الخاص بها، حيث وجد نفسه أمام كم هائل من الأشرطة والاقراص الممغنطة التي لا يدري عنها شيئا أو يعرف محتوياتها أو لديه القدرة على فحصها ومعرفة مضمونها، مما اضطر إلى مغادرة مركز حاسب الشركة المنافسة خالي الوفاض ومع أن الشركة المناسبة قامت من تلقاء نفسها بعد ذلك بعدة أيام بتسليم بيانات العناوين إلى الشركة المجني عليه إلا أنه من الوارد بالتأكيد – أن تكون الاشرطة المعنية قد تم استنساخها قبل تسليمها ، وهو ما يكون قد افقد امر المحكمة جدواها. راجع

31- Lister, Martin. Dovey, Jon. Giddings, Seth. Grant, Iain. Kelly, Kieran. (January 29, 2009) New Media: A Critical Introduction, USA/UK Europe : Routledge; 2 edition.

لمكافحة الغش المعلوماتى بالنمسا بأن شيئا ما فى نظام تشغيل حاسب الفاعل قد جرى تغييره وقيامهم بناء على ذلك باستنساخ الأقراص المغنطة المضبوطة عن طريق أنظمة حاسباتهم[١].

(جـ) صعوبة الوصول إلى الدليل

تحاط البيانات المخزنة الكترونيا أو المنقولة عبر شبكات الاتصال بجدار من الحماية الفنية لإعاقة محاولة الوصول غير المشروعة إليها للاطلاع عليها أو استنساخها[٢].. كذلك يمكن للمجرم المعلوماتى أن يزيد من صعوبة عملية التفتيش التى قد تباشر للحصول على الأدلة التى تدينه عن طريق مجموعة من الإجراءات الأمنية كاستخدام كلمة السر للوصول إليها أو دس تعليمات خفية بينها أو ترميزها لإعاقة أو منع الاطلاع عليها أو ضبطها . لذا فإن استخدام تقنيات التشفير لهذا الغرض يعد إحدى العقبات الكبرى التى تعوق رقابة البيانات المخزنة أو المنقولة عبر حدود الدولة والتى تقلل من قدرة جهات التحرى والتحقيق والملاحقة على الاطلاع عليها الأمر الذى يجعل حماية حرمة البيانات الشخصية المخزنة فى مراكز الحاسبات والشبكات أو المتعلقة بالأسرار التجارية العادية والالكترونية أو بتدابير الأمن والدفاع أمرا بالغ الصعوبة[٣].

---

(١) راجع في ذلك : د. هشام محمد فريد رستم ، مرجع سابق، ص٣٥-٣٦

(٢) تواجه عملية جمع الأدلة الاليكترونية واستعمالها بعض التحديات الرئيسية major challenges ومنها :

- صعوبة الوصول إلى الملفات المحذوفة أو المخبأة أو المحمية بموجب كلمات مرور داخل النظم الضخمة المرتبطة من خلال الشبكات.
- صعوبة استعادة البيانات من بعض الوسائل أو الوسائط القديمة.
- صعوبة العثور على الملفات او السجلات المحورية من بين المجالات الشاسعة للبيانات (مثال : سجلات البريد الالكتروني)
- صعوبة تحليل صحة الملفات – ومعرفة ما إذا كان قد تم تعديلها او محوها :

راجع في ذلك :

Linda volonino ph. D.ibid., p.14

(٣) انظر في ذلك :

يشير الأستاذ sieber بأن مشاكل عديدة لا يستهان بها قد نجمت من استخدام الجناة في بعض الجرائم المعلوماتية التي وقعت بالمانيا الاتحادية سابقا لتقنيات التشفير أو الترميز

وتصطدم عقبة الوصول إلى الدليل المعلوماتى بمشكلة إجرائية تتعلق بمدى سريان القيود الخاصة بضبط الأوراق على ضبط محتوى نظام المعالجة الآلية للبيانات والمحمى فنيا فى مواجهة الاطلاع غير المسموح به حيث يحظر قانون الإجراءات الجنائية المصري والإماراتى بمقتضى المادتين ٥٢، ٥٨ على التوإلى [(١)]. اطلاع مأمور الضبط القضائي على الأوراق المختومة أو المغلقة[(٢)]. الموجودة فى منزل المتهم أثناء تفتيشه[(٣)].وعلة ذلك الحفاظ على الآثار التى تتضمنها الأوراق وهنا يثور تساؤل عما إذا كان حكم هاتين المادتين واجب الإتباع بالنسبة لإطلاع مأمور الضبط القضائى على محتوى نظام المعالجة الآلية للبيانات من عدمه وذلك فى حالة ما إذا كان محاطا بجدار من الحماية الفنية تعوق الاطلاع عليه. ونبادر بالإيجاب على هذا التساؤل استنادا إلى سببين:

الأول: أن السبب الذى من أجله تم تقرير هذا الحكم بالنسبة للأوراق المختومة أو المغلقة يتوافر أيضا بالنسبة لمحتوى نظام المعالجة الآلية للبيانات المحمى فنيا ضد الإطلاع غير المسموح به. فحظر المشرع اطلاع مأمور الضبط القضائى على هذه الأوراق إنما هو لمظنة أن الغلق أو التغليف يضفى عليها مزيدا من السرية ويفصح عن رغبة صاحبها فى عدم اطلاع الغير على مضمونها بغير إذنه وهو ما يتحقق فى البيانات المخزنة أو المنقولة عبر نظام أو شبكة حاسب إذا كانت محمية فنيا ضد الاطلاع غير المسموح به . فمحتوى النظام لا

لإعاقة اكتشاف أو الوصول إلى أدلة تدينهم وبوجه خاص في مجال وسائل التخزين التي يكون صعبها ضبطها.

راجع في ذلك : Ulrich Sieber Ibid, p. 141

(١) تنص المادة الأولى منهما على أنه " إذا وجدت في منزل المتهم أوراق مختومة أو مغلقة بأية طريقة فلا تجوز لمأمور الضبط القضائي أن يفضها ، وبذات الصياغة تقريبا يسري نص المادة ٥٨ أ.ج. إماراتي .

(٢) فإذا كانت ظاهرا أن التغليف لا ينطوي وإنما يحوي جسما صلبا، فإنه يجوز لمأمور الضبط القضائي فض الغلاف لفحص محتوياته نقض مصري ٢٤ يونية ١٩٥٨ ، مجموعة أحكام النقض س٩ رقم ١٨٠ ص٧١٦.

(٣) قضى في مصر بعدم دستورية المادة ٤٧ من قانون الإجراءات الجنائية المصري في ٢ يونيه ١٩٨٤ ومن ثم لم يعد هناك مجال لتطبيق نص المادة ٥٢ من هذا القانون في حالة التلبس بالجريمة.

يكون بذلك مكشوفا بل محجوبا عن الغير حيث لا يتاح الوصول والاطلاع عليه بغير معرفة طريق ومفاتيح وكود التشغيل [١].

الثانى:أن المادة ٥٢ إجراءات مصرى (٥٨ إجراءات إماراتى) تضع قاعدة عامة لضمان الأسرار التى تحتويها سائر وسائط وأوعية حفظ وتخزين ونقل المعلومات سواء ما كان منها تقليديا كالأوراق أو مستحدثا كالأقراص المرنة والأشرطة المغنطة والذاكرات الداخلية للحاسبات وشبكات المعلومات المحلية والإقليمية والعالمية.

والجدير بالإشارة إليه أن كلا من التشريعين الإجرائيين المصرى والإماراتى لا ينفرد بهذه النتيجة بل يشاركهما فيها العديد من القوانين ومنها على سبيل المثال قانون الإجراءات الجنائية الالمانى ، فطبقا للمادة ١١٠ منه تقتصر سلطة الاطلاع على مخرجات الحاسب وغيرها من دعائم البيانات على المدعى العام وحده ، ولا يكون لضباط الشرطة حق الاطلاع على البيانات عن طريق تشغيل البرامج أو الاطلاع على ملفات البيانات المخزنة داخل الحاسب بغير إذن من له حق التصرف فيها ، ومالهم قانونا هو فحص دعائم البيانات عن طريق النظر فحسب دون استخدام مساعدات فنية[٢].

(د) افتقاد الآثار المؤدية إلى الدليل

يحدث فى بعض الأحيان إدخال البيانات مباشرة فى نظام الحاسب دون تطلب وجود وثائق معاونة (وثائق خاصة بالإدخال) كما هو الحال فى بعض نظم العمليات المباشرة التى تقوم على استبدال الإذن الكتابى لإدخال البيانات بإجراءات أخرى تعتمد على ضوابط للإذن متضمنة فى برنامج الحاسب (مثل المصادقة على الحد الأقصى للإئتمان وفى مجال العمليات المالية قد يباشر الحاسب بعض العمليات المحاسبية بغير الحاجة إلى ادخال كما هو الحال لإحتساب الفائدة على الإيداعات البنكية وقيدها آليا بأرصدة حسابات العملاء على أساس الشروط المتفق عليها مسبقا والموجودة فى برنامج الحاسب.

---

(١) راجع في ذلك :

د. هشام محمد فريد رستم، سابق الإشارة إليه ص٣٤.

(٢) انظر في ذلك :

Manfred Mothren schlager, computer crimes and other crimes against information technology in Bermany , rev, inter, D.P. leret 2e trimesters 1993,p.351

ويكون من السهل فى كل من هذين النوعين من العمليات ارتكاب بعض أنواع من الجرائم كاختلاس المال والتزوير بإدخال بيانات غير معتمدة فى نظام الحاسب أو تعديل برامجه أو البيانات المخزنة داخله دون أن يترتب على ذلك أى أثر يشير إلى حدوث هذا الادخال أو التعديل . لذا يتعين على المحقق إزاء صعوبة الوصول إلى مرتكبى الجرائم فى كلا هذين النوعين من العمليات وعدم ترك التغيرات فى البرامج أو البيانات آثار كتلك التى يخلفها التزوير المادى فى المحررات التقليدية[١]. أن يسعى لتحديد دائرة الأشخاص القائمين أو المتصلين فى عمليات إدخال ومعالجة البيانات وغيرها من عمليات التسجيل[٢]. مع الاستفادة من ضوابط الرقابة التى تباشر فى النظام المعلوماتى على الإدخال والمعالجة اضافة إلى تتبع الأموال المختلفة إن وجدت باعتبارها محصلة الجريمة التى يستولى عليها المجرم فى نهاية الأمر[٣].

ثالثا: المعوقات الخاصة بالعامل البشرى Human Factor

ويتعدد هذا النوع من المعوقات على النحو التإلى:

أ- مكان ارتكاب الجريمة

يتم ارتكاب جريمة الذكاء الاصطناعي (A.I) عادة عن بعد حيث لا يتواجد الفاعل على مسرح الجريمة ومن ثم تتباعد المسافات بين الفعل (من خلال حاسب الفاعل) و النتيجة (المعطيات محل الاعتداء) وهذه المسافات لا تقف عند حدود الدولة بل قد تمتد إلى النطاق الإقليمى لدول أخرى مما يضاعف صعوبة كشفها أو ملاحقتها[٤]. فقد أعلنت السلطات البريطانية أن أكثر من عشرة آلاف اسطوانة تعليمية عن الإيدز قد أدخلت إلى المستشفيات فى كل من بريطانيا والسويد والدنمارك والنرويج. وقد اكتشفت أجهزة البيانات أنها مصابة بفيروس "نورجان "

---

(١) راجع في ذلك :

Jack Bologena corporate faraud : the Basice of prevention and detection , Butterworth publishers 1984,p.75

(٢) راجع في ذلك :

J.Tappolet , La fracuc infromatieque, rev, int , crim poltech 1988,p.351

(٣) راجع في ذلك : د. هشام محمد فريد رستم ، سابق الإشارة إليه ص٣١.

(٤) راجع في ذلك : د. أسامة محمد محي الدين عوض، جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات ، بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة ٢٥-٢٨ أكتوبر ١٩٩٣.

وهو فيروس يؤدى إلى تخريب أجهزة الحاسب الآلي الشخصى- وإتلاف البرامج التى تعمل عليه وفى غضون ذلك. بدأت شرطة سكوتلانديارد تحقيقات واسعة النطاق فى هذه القضية باعتبارها جريمة تخريب وقد أثبتت التحقيقات مايلى:

(أ) أن هذه الاسطوانة وصلت إلى الأشخاص بالبريد من مصادر مختلفة بهدف تخريب البرامج المرسلة إليهم وأن أسماء الذين وجهت لهم الاسطوانات يبلغ عددهم نحو سبعة آلاف شخص قد تم بيعها إلى شركة تدعى " كيتيما " وهى مؤسسة تخص رجل أعمال كينى " يدعى كيتيما " وقد اتضح أن قائمة الأسماء التى أحضرت معه خلال زيارته لبريطانيا فى الفترة من ٣١ أكتوبر حتى ٣٠ نوفمبر ١٩٨٩ ولكنه لم يستدل له على عنوان.

(ب) أن عددا من هذه الاسطوانات ظهرت فى كاليفونيا وفى بلجيكا وزيمبابوى.

(ج) الرسائل أرسلت مع رسائل معنونة بـ "معلومات عن الإيدز " لكن تبين أنها تحتوى على فيروس نورجان الذى يهاجم أجهزة الحاسب الشخصى من نوع I . B . M والمتوافقة معه.

(د) تسأل الرسالة المرفقة مع الاسطوانة عن رسوم ملكية للبرنامج بمقدار ١٨٩ دولار أو ٣٧٨ دولارا حسب الطلب وإرسال الرد إلى عنوان فى بنما ولكن تبين أن معظم الرسائل أرسلت من لندن وبالتحرى تبين عدم وجود شركة بهذا الاسم ولا يوجد لها صندوق بريد فى بنما . بينما تبين أن مرسل الرسالة استخدام الاسم الأول من إحدى شركات البرامج الأمريكية العاملة فى بنما والتى أكدت عدم مسئوليتها عما حدث.

(و) تحذر الرسالة من أنه فى حالة عدم دفع الرسوم سيستخدم المرسل برنامجا لتخريب المعلومات ووقف جهاز الحاسب الآلي بشكل تلقائى ولكن ما أثار الانتباه إلى هذه القضية حدث خلال تحميل الاسطوانة وفقا لما قاله "جرسيرست" خبير الفيروسات ومستشار التطبيقات البريطانى [(١)].

ب- نقص خبرة الشرطة وجهات لادعاء والقضاء

يتطلب كشف جرائم الذكاء الاصطناعي (A.I) والوصول إلى مرتكبيها وملاحقتهم قضائيا استراتيجيات خاصة تتعلق بإكسابهم مهارات خاصة وعلى نحو

---

(١) راجع في ذلك :

د. أسامة محمد محي الدين عوض ، سابق الإشارة غليه ، ص٤٣٠ -٤٣١

يساعدهم على مواجهة تقنيات الحاسب الإلى المتطورة وتقنيات التلاعب به،حيث تنعقد وتتنوع التقنيات المرتبة بوسائل ارتكابها[١].

لذا يجب استخدام أساليب وتقنيات تحقيق جديدة ومبتكرة لتحديد نوعية الجريمة المرتكبة وشخصية مرتكبها وكيفية ارتكابها مع الاستعانة بوسائل جديدة أيضا لضبط الجانى والحصول على أدلة إدانته. إذ من المتصور أن يجد مأمورو الضبط القضائى أنفسهم غير قادرين على التعامل بالوسائل الاستدلالية والاجراءات التقليدية مع هذه النوعة من الجرائم [٢]. ومما يزيد من صعوبة هذا الأمر افتقار أنظمة الحاسبات وشبكات المعلومات فى البدايات الأولى لاستخدامها لأساليب الرقابة وضوابط التدقيق والمراجعة على العمليات والتطبيقات وعدم تزويدها بوسائل فنية لاكتشاف وتتبع مسار العمليات[٣] ، فضلا عن ما تصادفه هذه الجهات من صعوبات فى التحرى عن جرائم الحاسب عابرة الحدود لا سيما بعد انتشار استخدام شبكة المعلومات العالمية .

وكثيرا ما تفشل أجهزة الشرطة فى تقدير أهمية جريمة الذكاء الاصطناعي (A.I) نظرا لنقص الخبرة والتدريب[٤]. وللسبب ذاته أيضا كثيرا ما تفشل جهات التحقيق فى

---

(١)انظر في ذلك :

Donn, B., Parkar, vulnerabilities of EFT systm to intentionally causes losses in computers and Banking electronic funds transfer system and public poliecy edited by Kent w.colton and Keneth L. Kraemer, plenum press 1980,p. 97

(٢) جاء بتوصية المجلس الأوروبي رقم (٩٥) ١٣ في ١١ سبتمبر ١٩٩٥ في شأن مشاكل الاجراءات الجنائية المتعلقة بتكنولوجيا المعلومات ضرورة تشكيل وحدات خاصة لمكافحة جرائم الحاسب وإعداد برامج خاصة لتأهيل العاملين في مجال العدالة الجنائية لتطوير معلوماتهم في مجال تكنولوجيا المعلومات.

(٣) راجع في ذلك :

Bernard P. zajac Jr. police responses to computer crime in the united states the computer law and security report July – auyg 1985,pp.16-17

(٤) لقد علمت أن شابا طلب نسخة اسطوانة كمبيوتر وقام بتصوير البطاقة الملصقة عليها ثم قام بوضع الاسطوانة على السطح الزجاجي لآلة التصوير إلا أن الاستاتيكية التي نشأت عندما عملة الآلة أدت إلى مسح وإمالة كافة المعلومات المسجلة على الاسطوانة وهناك حالة أخرى حيث قام رجال الشرطة بوضع حقيبة كاملة تحتوي علىاسطوانات الكمبيوتر المصادرة وذلك

جمع أدلة جرائم الحاسب الآلي مثل مخرجات الحاسب وقوائم التشغيل ، بل إن المحقق كما هو الحال أحيانا فى بعض الجرائم الأخرى قد يدمر الدليل بمحوه الاسطوانة الصلبة من خطأ منه أو إهمال أو بالتعامل مع الأقراص المرنة أو بالتعامل المتسرع أو الخاطئ مع الأدلة[١].

ج- دور الخبراء فى فحص البيانات

يشكل الكم الهائل للبيانات التى يتم تداولها من خلال الأنظمة المعلوماتية أحد مصادر الصعوبات التى تعوق تحقيق جرائم الذكاء الاصطناعي (A.I) والدليل على ذلك أن طباعة كل ما يوجد على الدعامات الممغنطة لمركز حاسب متوسط الأهمية يتطلب مئات الآلاف من الصفحات والتى قد لا تثبت كلها تقريبا شيئا على الاطلاق. ويسلك المحقق غير المدرب لمواجهة هذه الصعوبة أحد سبيلين: إما حجز البيانات الالكترونية بقدر يفوق القدرة البشرية على مراجعتها أو التغاضى عن هذه البيانات كلها على أمل الحصول على اعتراف بالجريمة من المتهم[٢]. والواقع أنه بالامكان مواجهة هذة الصعوبة عن طريق أحد أمرين:

في صندوق السيارة بالقرب من جهاز الإرسال والاستقبال اللاسلكي فكانت النتيجة أن الإشارات الكهربائية القوية تسبب في تدميرها جميعا.

انظر في ذلك :

Burici sterling ibid, p. 208

وصرح مكتب التحقيقات الفيدرالي بأن خبارته لم يتمكنوا من تحديد ما إذا كان الحدث قد وقع بسبب عطل فني أو هجوم ماكر وقد حجب الموقع الخاص بشركة السمسمرة الوطنية والذي يرتاده ٢٠٠ ألف عميل لمدة تفوق الساعة – حاول خلالها مهندسوا الشركة الدفاع عن النظام ضد ما رأوا أنه هجوم . فقد لاحظوا مسئولوا الشركة أن الموقع كان يعمل ببطء شديد عند افتتاح السوق وهو الأمر الذي أدى إلى انخفاض إمكانية الوصول إليه إلى ٥٠%.

راجع في ذلك

D. voloninalinu ibid, p. 6

(١) انظر في ذلك :

Richard totta and antong hardcastle, computer related crime in information technology the law edited by chris Edwards and Nigel savage Macmillan publisher 1986,p.201

(٢) راجع في ذلك : د. هشام محمد فريد رستم، مرجع سابق ، ص٣٧

أ- الاستعانة بالخبرة الفنية لتحديد ما يجب دون سواه البحث عنه للإطلاع علية وضبطه واستعانة الجهات القائمة بالتحرى والتحقيق ، والحكم بالخبراء حين تتعامل مع الجرائم التى تقع فى مجال تكنولوجيا المعلومات تكاد تكون ضروره لاغنى عنها نظرا للطابع الفنى الخاص لأساليب ارتكابها والطبيعة المعنوية لمحل الاعتداء ونجاح هذه الجهات فى أداء رسالتها يتوقف إلى حد كبير علاوة على حسن اختيار الخبير على نجاحه فى المهمة التى عهد إليه بأدائها وموضوع هذه المهمة وإن كان يمكن للخبير نفسه أن يحدده إلا أن ذلك ليس مرغوبا فيه تجنبا لهيمنة دور الخبير على العملية الاثباتية وطغيانه على دور المحقق أو القاضى.

ب- الاستعانة بما تتيحه نظم المعالجة الآلية للبيانات من أساليب للتدقيق والفحص المنظم أو المنهجى ونظم ووسائل الإختبار والمراجعة.

رابعا: المعوقات الخاصة بالتنسيق الدولى فى مجال جمع الأدلة

هناك عقبات عديدة تقف بمنزلة حجر عثرة من أجل التنسيق الدولى فى مكافحة جرائم الذكاء الاصطناعي (A.I) وأبرزها ما يلى:

١- عدم وجود مفهوم عام مشترك بين الدول حتى الآن حول نماذج النشاط المكون للجريمة المتعلقة للحاسب الآلى .

٢- عدم وجود تعريف قانونى موحد للنشاط الإجرامي المتعلق بهذا النوع من الإجرام.

٣- انعدام التنسيق بين قوانين الاجراءات الجنائية للدول المختلفة فيما يتعلق بالتحرى والتحقيق فى الجريمة المعلوماتية. مع تعقد المشاكل القانونية والفنية الخاصة بتفتيش نظم المعلومات خارج حدود الدولة أو ضبط معلومات مخزنة فيه أو الأمر بتسليمها.

٤- عدم وجود معاهدات للتسليم أو للتعاون الثنائى أو الجماعى بين الدول تسمح بالتعاون الدولى أو عدم كفايتها إن وجدت لمواجهة المتطلبات الخاصة للجرائم المعلوماتية وسرعة التحريات فيها[١].

---

(١) لمواجهة هذه المشكلات أو بعضها، ناشد مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة المجرمين والذي عقد في هافانا عام ١٩٩٠ في قراره المتعلق بالجرائم ذات الصلة بالحاسب، الدول الأعضاء أن تكثف جهودها كي تكافح بمزيد من الفعاليات عمليات إساءة استعمال الحاسب التي تستدعي تطبيق جزاءات جنائية على الصعيد الوطني بما في ذلك النظر إذا

المبحث الرابع
إجراءات الضبط التشريعي في مجال
مكافحة جرائم الذكاء الاصطناعي (A.I)

أصبح لكل شخص يعيش في المجتمع الحق بالاتصال بغيره وتبادل المنافع المعنوية والمادية معه ليس فقط داخل دولته بل كذلك خارجها مع أبناء الدول الأخرى . وإذا كانت الدول قد استطاعت الحد من ذلك الاتصال والتبادل في أوقات مضت تحت

دعت الضرورة في أ – تحديث القوانين والإجراءات الجنائية بما في ذلك اتخاذ تدابير من أجل

١- ضمان أن الجزاءات والقوانين الراهنة بشأن سلطات التحقيق وقبول الأدلة في الاجراءات لاقضائية تنطبق على نحو ملائم وإدخال تغييرات مناسبة عليها إذا دعت الضرورة لذلك .

٢- النص على جرائم وجزاءات اجراءات تتعلق بالتحقيق والأدلة حيث تدعو الضرورة إلى ذلك للتصدي لهذا الشكل الجديد والمعقد من أشكال النشاط الإجرمي في حالة عدم وجود قوانين تنطبق على نحو ملائم. كما حث المؤتمر كذلك الدول الاعضاء على مضاعفة الأنشطة التي تبذلها على الصعيد الدولي من أجل مكافحة الجرائم المتصلة بالحاسبات بما في ذلك دخولها ، حسب الاقتضاء أطرافا في المعاهدات المتعلقة بتسليم المجرمين وتبادل المساعدات في المسائل الخاصة المرتبطة بالجرائم ذات الصلة بالحاسب وتصح القرار ذاته الدول الأعضاء بالعمل على أن تكون تشريعاتها المتعلقة بتسليم المجرمين وتبادل المساعدة في المسائل الجنائية منطبقة انطباقا كافيا على الأشكال الجدية للإجرام مثل الجرائم ذات الصلة بالحاسب وإن تتخذ خطوات محددة. حسب الاقتضاء من أجل تحقيق هذا الهدف وذلك بالإضافة إلى توصيات أخرى وقد يكون ملائمات كخطوة تعزز مسار التعاون الفعال وتكمل ما اتخذه مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة المجرمين في هذا لاشأن من قرارات أن يسفر بحث مؤتمرات الأمم المتحدة لموضوع الجرائم ذات الصلة بالحاسب عن فتح آفاق جديدة للتعاوةن الدولي في هذا المضمار لا سيما فيما يتعلق بوضع أو تطوير أ – معايير دولية لأمن المعالجة الآلية للبيانات ب – تدابير ملائمة لحل مشكلات الاختصاص القضائي التي تثيرها الجرائم المعلوماتية العابرة للحدود أو ذات الطبيعة الدولية جـ - اتفاقيات دولية تنطوي على نصوص تنظم اجراءات التفتيش والضبط المباشر الواقع عبر الحدود على الأنظمة المعلوماتية المتصلة فيما بينها والأشكال الأخرى للمساعدة المتبادلة مع كفالة الحماية في الوقت نفسه لحقوق وحرياتهم وسيادة الدول.

راجع في ذلك :

د. هشام محمد فريد رستم سابق الإشارة، ص ٤٩

ستار حماية متطلبات أمنها القومي والاقتصادي إذ إنها لم تعد كذلك في ظل عصر السماوات المفتوحة بفعل تقدم وسائل الاتصال عبر الأقمار الصناعية [١] ووسائط نقل الأخبار المعلوماتية عبر الأثير والموجات الكهرومغناطيسية لدرجة يمكن القول معها إن سيادة الدولة الإقليمية قد انحسرت عن الإقليم الفضائي أو الهوائي واقتصرت على إقليمها الأرضي والمائي فقط [٢] .

وقد كرست الأعمال القانونية الدولية حق الاتصال والحصول على المعلومات وتداولها ،وأكدت على أهمية ضمان ممارسته [٣]. فقد نص القرار ٥٩ الصادر عن الأمم المتحدة في ١٤ ديسمبر ١٩٤٦ على أن "حرية الاستعلام هي حق أساس للإنسان ،وهي حجر الزواية لكل الحريات التي كرست الأمم المتحدة نفسها للدفاع عنها،وحرية الاستعلام تشمل جمع ونقل ونشر المعلومات في كل دون عقبات ".

وتستلزم مثل هذه الجرائم وجود تعاون دولي فعال [٤] والذي يعد ضروريا من أجل حماية حقيقية لأنظمة الاتصالات البعدية التي تمر بالعديد من الدول وينشأ حتما عن وجود أوجه خلاف بين القوانين الوطنية والخاصة بتقنية نظم المعلومات

---

(١) راجع في ذلك :

Ravillon (Hume) les telecommunications par sateliet aspects juridiques Paris , ed, lifec 1997,

Mateesco – Matte (N) droit aerospatical les telcomunnications par natellites Pars , 1982

(٢) راجع في ذلك

Park 9K-G) la protection de la souverainet aerienne Paris, 1977

(٣) راجع في ذلك :

Pinto ® la Liberte d'infromation ed d'opinion en droit international , paris , L.G.D.J. 1984

(4) LA COmmision "invite fnstatment les autorites nationals compptentes a cooperer apin de parvenir a un accord international definissant les contenus illegaux et, par consequent, passibles de sanctions quelques soit le lieu de residence du fournisseur de contenu " et " propose Hume'etablissement de catalogues "nationaux " aisement accessibles recensant les contmis ou les operations illegales detectees sur intenrt ",

راجع في ذلك :

La criminamite infromatique sur L'internet

ما يعرف بالمعلومات المختبئة والذي ستكون لها نتيجة عكسية في صورة قيود وطنية على حرية حركة المعلومات.

وفي سبيل ذلك يمكن التعرض لأبرز الإجراءات الواجب إتباعها سعيا لمكافحة جرائم الذكاء الاصطناعي (A.I) وذلك على النحو التالي:

أولا: الإجراءات على المستوى المحلي والوطني

يمكن تقسيم هذه الإجراءات إلى نوعين أحدهما تدابير موضوعية والأخرى إجرائية . وذلك على النحو التالي :

١- الإجراءات الموضوعية (١)

من الأهمية بمكان مباشرة الإجراءات الآتية:

أ- يجب على كافة الدول أن تتبنى الإجراءات التشريعية وغيرها من الإجراءات اللازمة لإدراك عملية الدخول غير المشروع إلى سائر أو جزء من أجزاء نظام الحاسب الآلي كجريمة جنائية وفقا لأحكام قوانينها الوطنية إذا ما ارتكبت هذه الأفعال بصورة عمدية ويجوز لأي دولة أن تحدد من بين متطلبات ارتكاب الجريمة أن يكون ارتكابها من خلال اختراق تدابير الأمن أو بينة الحصول على بيانات الحاسب الآلي .

ب- ينبغي تبنى الإجراءات التشريعية وغيرها من الإجراءات اللازمة لإدراك أعمال الاعتراض دون حق والتي تتم بأساليب فنية كعمليات نقل الحاسب الآلي إلى أو من خلال حاسب آلي آخر وكذا الاشارات الالكترومغناطيسية الصادرة من أحد نظم المعلومات والتي تحمل مثل تلك البيانات واعتبارها جريمة جنائية لأحكام قوانينها الوطنية إذا ما ارتكبت بصورة عمدية .

ج- يجب على الدول أن تتبنى الإجراءات التشريعية اللازمة لإدراك أعمال الإضرار أو المحو أو الاتلاف أوالتعديل أو الإعاقة التي تستهدف بيانات الحاسب الآلي بدون وجه حق واعتبارها جريمة إذا ما ارتكبت بصورة عمدية .

د- يجب على الدول أن تتبنى الإجراءات التشريعية اللازمة لإدراج أعمال الإعاقة الخطرة دون وجه حق بوظائف نظام الحاسب الآلي من خلال ادخال أو نقل أو

---

(١) راجع في ذلك

European committee on crime problems 9cppc). Committee of experts on crime in cyber – space (pc-cy) draft convention on cybercirm 9draf N19) stansbourg, 25 April 2000

الإضرار أو محو أو اتلاف أو تعديل أو اعاقة بيانات الحاسب الآلي وادراكها باعتبارها جريمة جنائية إذا ارتكبت بصفة عمدية .

هـ -يجب على الدول أن تتبنى الإجراءات التشريعية اللازمة لامكانية مساءلة الأشخاص المعنوية جنائيا عن الجرائم الناشئة عن نظم المعلومات وذلك في الأحوال التي يؤدي فيها قصور الاشراف أو الرقابة من قبل الشخص الطبيعية إلى تسهيل ارتكابها.

٢- الإجراءات الاجرائية [١]

وتتمثل هذه الإجراءات على النحو التالي :

أ- يجب على الدول أن تتخذ الإجراءات التشريعية التي تخولها سلطة تفتيش ما يلي:

(١)أحد أنظمة الحاسب الآلي أو جزء منه وبيانات الحاسب الآلي المختزنة به .

(٢)أحد الوسائط التي قد تكون بيانات الحاسب الآلي مختزنة به ،وذلك في أراضيها أو في أحد الأماكن الأخرى التي تمارس عليها سلطاتها لأغراض التحقيق .

ب- يجب على الدول أو تتخذ الإجراءات التشريعية اللازمة لتخويل سلطاتها المعنية في اصدار الأمر لأي شخص سواء كان متواجدا في إقليمها في أي مكان آخر عليه سلطاتها السيادية لكي يقدم أي بيانات محددة واقعة تحت سيطرته ومخزنة في أحد أنظمة الحاسب الآلي أو أحد الوسائط المستخدمة في تخزين البيانات وذلك بالصورة التي تطلبها تلك السلطات لأغراض التحقيق.

ج- يجب على الدول أن تتبنى الإجراءات التشريعية اللازمة لتمكين سلطاتها المعنية من الحصول على نسخة حفظ سريعة للبيانات المخزنة في أحد نظم الحاسب الآلي وذلك لأغراض التحقيقات وذلك إذا تبين أنها معرضة بصفة خاصة للفقد والتعديل .

د- يجب على الدول أن تتبنى الإجراءات التشريعية اللازمة لإجبار الشخص الذي تتخذ حياله إجراءات الحفظ المشار إليها سلفا على الاحتفاظ بسرية الاجراءات لمدة محددة من الزمن وفقا للإطار الذي يسمح به القانون الوضعي .

---

(١) راجع في ذلك

Europan committee on crime problems (cppc) committee of experts on rime in cyber – space (pc – cy0 draft convention on cyber crimd (draft N 10) Strasbourg 25 april 2000

هـ- يجب على الدول أن تتخذ الإجراءات التشريعية اللازمة التي تكفل حفظ بيانات النقل والخاصة بأحد الاتصالات المحددة كما تكفل الحفظ السريع لتلك البيانات الخاصة بعملية النقل وبغض النظر إذا كان مقدم الخدمة واحدة أو أكثر ممن شاركوا في عملية نقل هذا الاتصال .

و- يجب على الدول أن تتخذ الإجراءات التشريعية اللازمة لمد اختصاصها القضائي على أي من الجرائم المشار إليها إذا ما ارتكبت بصورة كليه أو جزئية على أراضيها أو على متن باخرة أو طائرة أو قمر صناعي يحمل علمها أو مسجل لديها. أو من قبل أحد مواطنيها إذا كانت الجريمة من الجرائم المعاقب عليها وفقا لأحكام القانون الجنائي الساري في محل ارتكابه أو إذا كانت الجريمة قد ارتكبت خارج الاختصاص الإقليمي لأي دولة .

ثانيا: الإجراءات الواجب اتباعها على المستوى العربي

نظرا لظهور مشكلة جرائم الذكاء الاصطناعي (A.I) بوصفها مشكلة أمنية ، وقانونية واجتماعية ، فان خبراء الأمن المعلوماتي وصانعي السياسات الحكومية ومسوقي الحاسب الآلي ، والأفراد المهتمين في هذا الموضوع بحاجة إلى تغيير نظرتهم تجاه جرائم الحاسب الآلي ، ليس لأنها مشكلة وطنية فقط، وإنما كمشكلة عالمية ،وتتطلب الإجراءات الوطنية تعاونا في مجال القطاعين العام والخاص،فعلى القطاع الخاص الالتزام بإجراءات الوقاية، وعلى القطاع العام تنفيذ الإجراءات اللازمة لمكافحة الجريمة ،وبوجه عام هناك حاجة إلى تحقيق ما يلي على المستوى العربي:

١-وجود التشريعات اللازمة لحماية ملكية الحاسب الآلي، وللبيانات،والمعلومات والمعدات اللازمة للتشغيل والتوصيل.

٢-زيادة الوعي الوطني في عالمنا العربي لجرائم الذكاء الاصطناعي (A.I) وللعقوبات المترتبة عليها.

٣-إنشاء وحدات مختصة في التحقيق في جرائم الذكاء الاصطناعي (A.I) في المحاكم والشرطة.

٤-إيجاد نوع من التعاون العربي في الحماية والوقاية من هذه الجرائم.

ومن ثم فإن الإجراءات والإجراءات الواجب إتباعها تكون على النحو التالي:

١-مساءلة الأشخاص الطبيعيين والأشخاص المعنويين والمؤسسات الفردية إذا اقترنت الجريمة لصالح الأشخاص والمؤسسات أو بأسمائها بالإضافة إلى مساءلة الأشخاص الطبيعيين من مقترفيها وشركائهم.

٢-إدماج نصوص جرائم الذكاء الاصطناعي (A.I) في قانون العقوبات الوطني على أن يفرد لها فصل خاص.

٣-تدريب رجال الشرطة القضائية ورجال التحقيق والقضاء على كيفية استخدام أجهزة المعلومات وأدواتها وأشرطتها وآلات الطباعة الخاصة بها والإحاطة بكيفية إساءة استخدامها.

٤-تدريب رجال الشرطة القضائية والتحقيق والقضاء على كيفية الكشف عن هذه الجرائم وإثباتها.

٥-حث الدول على التعاون فيما بينها خاصة في مجال المساعدات والإنابة القضائية للكشف عن هذه الجرائم، وجمع الأدلة لإثباتها ، وتسليم المجرمين المقترفين لها، وتنفيذ الأحكام الأجنبية الصادرة بالإدانة والعقوبة على رعايا الدولة المقترفين لها بالخارج.

ثالثا: الإجراءات الواجب مباشرتها على المستوى الدولي [(١)]

أ- يجب على الدول أن تقدم لبعضها البعض المعونة المتبادل وذلك بأكبر قدر ممكن لأغراض التحقيق والاجراءات الخاصة بالجرائم الجنائية المتعلقة بنظم الذكاء الاصطناعي (A.I).

ب- يجب على الدول أنتقبل وتستجيب إلى طلبات المعونة المتبادلة من خلال وسائل الاتصال السريعة كالفاكس والبريد الالكتروني ،بالقدر الذي يوفر للطرف الطالب المستوى من الأمن والمصادقة.

ج- تخضع المعونة المتبادلة للاشتراطات المنصوص عليها في قوانين الدولة المدعية أو المنصوص عليها بموجب اتفاقيات المعونة المتبادلة .

---

(١) راجع في ذلك

Europan committee on crime problems (cppc) committee of experts on rime in cyber – space (pc – cy0 draft convention on cyber crimd (draft N 19) Strasbourg 25 april 2000

د- في الأحوال التي يسمح فيها للطرف المدعي عليه بتعليق طلب المعونة المتبادلة على اشتراط وجود جريمة مزدوجة ،يعتبر هذا الشرط محل اعتبار وبغض النظر عما إذا كانت قوانين هذه الدولة تضع الجريمة في نطاق ذات تصنيف آخر .

هـ- تحدد كل دولة سلطة مركزية تنهض بالمسئولين إرسال طلبات المعونة المتبادلة والرد عليها وتنفيذها أو نقلها للسلطات المعنية للتنفيذ.

و- تنفذ طلبات المعونة المتبادلة وفقا للاجراءات التي يحددها الطرف المدعي فيما عدا الأحوال التي لا تتصل فيها تلك الاجراءات مع أحكام القانون السائد بالدولة المدعى عليها .

ز- يجوز للدولة المدعي عليها أن ترفض طلب المعونة إذا ما توافرت لديها القناعة بأن الالتزام بما ورد بالطلب قد يخل بسيادتها أو أمنها أو نظامها العام أو بأي من مصالحها الأساسية الأخرى.

ح- يجوز للدولة المدعي عليها تأجيل التصرف في الطلب إذا كان هذا التصرف سيخل بالتحقيقات أو اجراءات الادعاء أو الاجراءات الجنائية التي تباشر بمعرفة السلطات المعنية .

ط- يجب على الدول المدعي عليها أن تخطر الدولة المدعية بصورة فورية بنتائج تنفيذ طلب المعونة فإذا ما رفض الطلب أو تم تأجيله يجب تقديم الأسباب إلى الرفض أو التأجيل .

ى- يجوز للدولة المدعية أن تطلب من الدولة المدعي عليها أن تحتفظ بسرية الوقائع والمحتويات التي يتضمنها الطلب ،فإذا لم يكن بمقدور الدولة المدعية عليها الوفاء بمتطلبات سرية الطلب فيجب عليها اخطار الدولة المدعية بذلك وعلى الاخيرة في هذه الحالة تحديد ما إذا كان سينفذ الطلب من عدمه .

ك- يجوز في حالة الاستعجال ارسال طلبات المعونة المتبادلة مباشرة إلي السلطات القضائية بما فيها النيابة العامة لدى الدولة الدعية عليها وفي مثل الحالة يجب ارسال نسخة بنفس الطلب إلى السلطة المركزية القائمة لدى الدولة المدعي عليها.

خاتمة الدراسة

تناولنا فى هذا البحث جرائم الذكاء الاصطناعي (A.I) والتي انتشرت بشكل كبير، وترتب على هذا الانتشار أضرارا بالغة فى حق الأفراد والمؤسسات بل والدول ذاتها، فمنظومة الأمن القومى لأى من الدول قد يخترقها الذكاء الاصطناعي (A.I)، فضلا عن ذلك فجرائم الذكاء الاصطناعي (A.I) تأتى على أشكال وتصنيفات متنوعة، ولاشك أن جريمة الذكاء الاصطناعي (A.I) ليست حكرا على بعض الدول دون الأخرى، إذ إن الواقع الذى يفرضه التقدم التكنولوجى والمعلوماتى والذى أكده التطور المستمر فى وسائل معالجة ونقل المعلومات باعتبارها باتت المحدد الاستراتيجي للبناء الثقافي والإنجاز الاقتصادي، يؤكد أن هذه الجريمة الجديدة، آخذة فى الانتشار فى ربوع الأرض. وأمام هذا الانتشار الكبير لهذا النوع من الجرائم اتجهت الدول إلى تضمين أنظمتها القانونية قوانين لمكافحة جريمة الذكاء الاصطناعي (A.I) من أجل إنزال حكم القانون على المجرم المعلوماتى أينما وجد وتوقيع العقاب عليه. فضلا عن اتجاه الكثير من الدول إلى تفعيل مبدأ التعاون الدولى فى مجال مكافحة جرائم الذكاء الاصطناعي (A.I).

ويؤكد الكثير من رجال القانون على ضرورة إنشاء محكمة إلكترونية لسد الفجوة القانونية التي أحدثها التطور التكنولوجي الهائل في مجال الذكاء الاصطناعي (A.I)، فهناك جرائم ترتكب، وحرمات تنتهك، وحقوق تسلب عبر تطبيقات الذكاء الاصطناعي (A.I) دون رقابة قانونية تذكر، والسبب في ذلك عدم وجود قانون دولي رادع يلاحق إجرام الذكاء الاصطناعي (A.I)، إلا أن ذلك ليس من الأمور البعيدة التي يمكن أن تشق طريقها إلى التطبيق العملي في المستقبل القريب.

وغنى عن البيان أن الدول العربية ليست ببعيدة عن مرمى جرائم الذكاء الاصطناعي (A.I)، ذلك أن هذه الجرائم لم تترك بلدا من بلاد العالم إلا واخترقتها ونالت من أهداف محدده فيها، هذا ويلزم للمجتمع المعلوماتى فى مجال قانون الاجراءات الجنائية أن ينشئ قواعد قانونية حديثة بحيث تضع معلومات معينة تحت تصرف السلطة المهيمنة على التحقيق فى مجال جرائم الذكاء الاصطناعي (A.I).

نتائج الدراسة

يمكن تحديد ابرز نتائج الدراسة على النحو التالي:

أولا: تعد جرائم الذكاء الاصطناعي ذات بعد دولي، إذ إن الواقع الذى يفرضه التقدم التكنولوجى والمعلوماتى والذى أكده التطور المستمر فى وسائل معالجة ونقل المعلومات باعتبارها باتت المحدد الاستراتيجي للبناء الثقافي والإنجاز الاقتصادي، يؤكد أن هذه الجريمة الجديدة، آخذة فى الانتشار فى ربوع الأرض

ثانيا: لقد سعت التشريعات المقارنة إلى تضمين أنظمتها القانونية قوانين لمكافحة جرائم الذكاء الاصطناعي من أجل إنزال سيادة القانون واحداث الضبط التشريعي لتلك الجرائم.

ثالثا: يظهر مدى خطورة جرائم الذكاء الاصطناعي، فهي تطال الحق في المعلومات، وتمس الحياة الخاصة للأفراد، وتهدد الأمن القومي والسيادة الوطنية، وتشيع فقدان الثقة بالتقنية وتهدد إبداع العقل البشري

رابعا: لا تبدو قوانين الجزاء المقارن في حالتها الراهنة كافية أو فعالة على النحو المطلوب أو المرضي فنصوصها والنظريات والمبادئ القانونية التي تتضمنها أو تقف وراءها موروث بعضها من القرن ١٩ حيث لم يكن هناك تقنيات أو ذكاء اصطناعي وهو الأمر الذي يتطلب فعالية التشريعات تجاه جرائم الذكاء الاصطناعي.

توصيات الدراسة

على أية حال فإنه فى سبيل الحد من جرائم الذكاء الاصطناعي (A.I)، فيجب أن نضع فى الاعتبار المقترحات والحلول اللآتية:-

١- ضرورة تقنين قواعد جديدة لمكافحة جرائم الذكاء الاصطناعي (A.I) ؛ تأخذ بعين الاعتبار الطبيعة الخاصة لهذه الجرائم ولاسيما فيما يتعلق بالإثبات في الدعاوى الناشئة عن هذه الجرائم ؛ سواء في ذلك الدعاوى الجنائية والمدنية والتأديبية. كما ينبغي تعديل قواعد الإجراءات الجنائية لتتلاءم مع هذه الجرائم.

٢- ضرورة التنسيق والتعاون الدولي قضائيا وإجرائيا في مكافحة جرائم الذكاء الاصطناعي (A.I).

٣- ضرورة تخصيص شرطة خاصة لمكافحة جرائم الذكاء الاصطناعي (A.I) ؛ وذلك من رجال الشرطة المدربين على كيفية التعامل مع أجهزة الحاسب الآلي (Computer) والإنترنت (Internet).

٤- يتعين تدريب وتحديث رجال الادعاء العام – أو النيابة العامة – والقضاء بشأن التعامل مع أجهزة الحاسب الآلي (Computer) والإنترنت (Internet) .

٥- ينبغي أن تنص التشريعات العربية-مثلا- على اعتبار أن الإنترنت (Internet) يعد وسيلة من وسائل العلانية في قانون العقوبات والقوانين ذات الصلة بجرائم الذكاء الاصطناعي (A.I) ؛ مع الأخذ بعين الاعتبار أن الإنترنت (Internet) أوسع انتشارا من سائر وسائل النشر والعلانية الأخرى .

٦- يلزم تعديل قوانين ونظم الإجراءات الجزائية (الجنائية) ؛ بالقدر الذي يسمح ببيان الأحكام اللازم اتباعها حال التفتيش على الحاسبات وعند ضبط المعلومات التي تحتويها وضبط البريد الإلكتروني حتى يستمد الدليل مشروعيته .

٧- يلزم أن تمتد إجراءات التفتيش إلى أية نظم حاسب آلي أخرى ؛ يمكن أن تكون ذات صلة بالنظام محل التفتيش وضبط ما بها من معلومات. ويشترط في هذه الحالة أن يكون هذا الإجراء ضروريا، والقاعدة العمة – في هذا الشأن – الضرورة تقدر بقدرها .

٨- يتعين أن تكون للسلطات القائمة بالضبط والتفتيش : سلطة توجيه أوامر لمن تكون لديه معلومات خاصة للدخول على ما يحويه الحاسب الآلي والإنترنت (Internet) من معلومات للإطلاع عليها .

٩- ضرورة النص صراحة في القوانين المنظمة للإثبات – الجنائي والمدني – بما يسمح للقاضي بأن يستند إلى الأدلة المستخرجة من الحاسب الآلي والإنترنت (Internet) في الإثبات ؛ طالما أن ضبط هذه الأدلة جاء وليد إجراءات مشروعة، على أن تتم مناقشة هذه الأدلة بالمحكمة وبحضور الخبير؛ وبما يحقق مبدأ المواجهة بين الخصوم .

١٠- إنشاء قسم جديد بكليات الحقوق بالجامعات العربية لدراسة الحماية القانونية لتطبيقات الذكاء الاصطناعي (A.I) أو تحت مسمى آخر "قانون المعلوماتية و الذكاء الاصطناعي (A.I) ".

١١- أن تسعي الدول العربية إلى إنشاء منظمة عربية تهتم بالتنسيق في مجال مكافحة جرائم الذكاء الاصطناعي (A.I)؛ مع تشجيع قيام إتحادات عربية تهتم بالتصدي لجرائم الذكاء الاصطناعي (A.I) وتفعيل دور المنظمات والإدارات والحكومات العربية في مواجهة هذه الجرائم عن طريق نظام الأمن الوقائي، ويكون من الأفضل إنشاء شرطة عربية تهتم بمكافحة جرائم الذكاء الاصطناعي (A.I).

المراجع

أولا: باللغة العربية:

١- الكتب

١) د. أبو اليزيد على المتيت، الحقوق على المصنفات الأدبية والفنية والعلمية، منشأة دار المعارف، الإسكندرية، الطبعة الأولى ١٩٩٧.

٢) د. أحمد فتحى سرور، الوسيط فى قانون العقوبات، القسم الخاص، القاهرة، دار النهضة العربية، ٢٠١٠.

٣) آمنة على يوسف، قراصنة أنظمة الحاسب الآلي، المؤتمر القومى الثالث عشر لأمن الحاسب الآلي، ، القاهرة، ١٩٩٩

٤) انتصار نورى الغريب، أمن الحاسب الآلي والقانون٠ دار الراتب العالمية ، لبنان،١٩٩٤.

٥) د. جلال أحمد خليل، النظام القانونى لحماية الاختراعات ونقل التكنولوجيا إلى الدول النامية، جامعة الكويت،١٩٩٢.

٦) د. جميل عبد الباقى الصغير، القانون الجنائى والتكنولوجيا الحديثة، الكتاب الأول، الجرائم الناتجة عن استخدام الحاسب الإلى ، الطبعة الأولى، دار النهضة العربية، ١٩٩٢.

٧) حسن عماد مكاوي، ليلى حسين، الاتصال ونظرياته المعاصرة، القاهرة، الدار المصرية اللبنانية، الطبعة الرابعة، أكتوبر ٢٠١٣

٨) سليم خالد، ثقافة مواقع التواصل الاجتماعي والمجتمعات المحلية، دار المتنبي للنشر والتوزيع، قطر، ٢٠٠٥.

٩) شريف اللبان ، تكنولوجيا الاتصال. المخاطر والتحديات والتأثيرات الإجتماعية، القاهرة، الهيئة المصرية العامة للكتاب، ٢٠٠٨

١٠) د. طارق سرور، ذاتية جرائم الإعلام الإلكتروني (دراسة مقارنة)، القاهرة، دار النهضة النهضة العربية .٢٠٠١

١١) د. عبد الحميد الجمال، مبادئ القانون الكتاب الثانى، العلاقات القانونية، الفتح للطباعة والنشر، الإسكندرية، ١٩٩٠.

١٢) د. عبد الرزاق السنهورى، الوسيط فى شرح القانون المدنى، القاهرة ١٩٩٩.

١٣) د. عبد العظيم مرسى وزير، شرح قانون العقوبات- القسم الخاص- جرائم الاعتداء على الأموال، دار النهضة العربية ١٩٩٣.

١٤) د.عبد الفتاح الصيفى، قانون العقوبات اللبنانى – جرائم الاعتداء على أمن الدولة وعلى الأموال، دار النهضة العربية، بيروت ١٩٧٢.

١٥) د. عبد المهيمن بكر، القسم الخاص فى قانون العقوبات، الطبعة السابعة ١٩٧٧.

١٦) د٠ عمر السعيد رمضان، شرح قانون العقوبات، القسم الخاص، دار النهضة العربية ١٩٧٥.

١٧) د. عمر الفاروق الحسينى، المشكلات العامة فى جرائم الحاسب الإلى وأبعادها الدولية، دراسة تحليلية نقدية بنصوص التشريع المصري مقارنا بالتشريع الفرنسى ، الطبعة الثانية،١٩٩٤.

١٨) د. عوض محمد، جرائم الأشخاص والأموال، دار المطبوعات الجامعية، الإسكندرية.

١٩) د. غانم محمد غانم، عدم ملائمة القواعد التقليدية فى قانون العقوبات لمكافحة جرائم الحاسب الآلي، مؤتمر القانون والحاسب الآلي والإنترنت (Internet)- الإمارات، مايو ٢٠٠٠.

٢٠) فتحي حسين عامر، وسائل الاتصال الحديثة من الجريدة إلى الفيس بوك، القاهرة، العربي للنشر والتوزيع، ٢٠١١

٢١) د. فوزية عبد الستار، شرح قانون العقوبات، القسم الخاص، دار النهضة العربية،١٩٨٣.

٢٢) د. ماجد عمار، المسئولية القانونية الناشئة عن استخدام فيروس برامج الحاسب الآلي ووسائل حمايتها، دار النهضة العربية، ٢٠٠٩

٢٣) د. محمد حسام لطفى، الحماية القانونية لبرامج الحاسب الآلي، دار الثقافة للطباعة والنشر. القاهرة ١٩٨٧.

٢٤) د.محمد سامى الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، القاهرة، دار النهضة العربية، الطبعة الثانية ٢٠١٥.

٢٥) د. محمد فهمى طلبه وآخرين، الحاسبات الالكترونية حاضرها ومستقبلها، موسوعة دلتا للكمبيوتر، مطابع الكتاب المصرى الحديث ١٩٩٢.

٢٦) د. محمد محيى الدين عوض، القانون الجنائى، جرائمه الخاصة ١٩٧٨/١٩٧٩.

٢٧) د. محمد مختار بربرى، قانون المعاملات التجارية، دار الفكر العربى، سنة ١٩٨٧.

٢٨) د.محمود محمود مصطفى، القسم الخاص، دار النهضة العربية، الطبعة الثامنة ١٩٨٤.

٢٩) د. محمود مصطفى القللى، شرح قانون العقوبات فى جرائم الأموال، الطبعة الأولى،١٩٣٩.

٣٠) د. محمود نجيب حسنى، جرائم الاعتداء على الأموال فى قانون العقوبات اللبنانى، دار النهضة العربية، بيروت

٣١) ـــــــــ، شرح قانون العقوبات، القسم الخاص، دار النهضة العربية، ١٩٨٨.

٣٢) مصطفى الجمال، مبادئ القانون، الكتاب الثانى، العلاقات القانونية، الفتح للطباعة والنشر، الإسكندرية،١٩٩٠.

٣٣) ميشال إنولا، تقنيات اتصال حديثة: الوسائط المتعددة وتطبيقاتها في الإعلام والثقافة والتربية، ترجمة: نصر الدين العياضي ورابح الصادق، باريس، دار الكتاب الجامعي، ٢٠٠٤.

٣٤) د. نبيل إبراهيم سعد، المدخل إلى القانون الكتاب الثانى، نظرية الحق، دار النهضة العربية، بيروت ١٩٩٥.

٣٥) نعوم تشومسكي، السيطرة على الإعلام.. الإنجازات الهائلة للبروباجندا، تعريب: أميمة عبد اللطيف، القاهرة، مكتبة الشروق الدولية، الطبعة الثانية، ٢٠٠٥

٣٦) د.هاني دويدار، نطاق احتكار المعرفة التكنولوجية بواسطة السرية، دار الجامعة الجديدة،١٩٩٦.

٣٧) د. هدى حامد قشقوش، جرائم الحاسب الالكتروني فى التشريع المقارن،القاهرة، دار النهضة العربية ١٩٩٢.

٣٨) د. هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة أسيوط ١٩٩٤.

٣٩) د. هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، القاهرة، دار النهضة العربية.٢٠٠٦

٢- الرسائل العلمية

١) د. خالد حمدي عبد الرحمن، الحماية القانونية للكيانات المنطقية، رسالة دكتوراة، حقوق عين شمس ١٩٩٢.

٢) د. عزة محمود أحمد خليل، مشكلات المسئولية المدنية فى مواجهة فيروس الحاسب. رسالة دكتوراة، جامعة القاهرة، كلية الحقوق، ١٩٩٤.

٣) عماد إبراهيم، أثر استخدام الفيس بوك على سلوك طلبة الجامعات، رسالة ماجستير غير منشورة، كلية التربية، جامعة عين شمس القاهرة، ٢٠٠٩.

٤) د. محمد محمد عنب، معاينة مسرح الجريمة، رسالة دكتوراة، أكاديمية الشرطة، كلية الدراسات العليا القاهرة ١٩٨٨.

٥) د. يونس خالد عرب مصطفى، جرائم الحاسب الآلي (Computer) دراسة مقارنة، رسالة ماجستير، الجامعة الأردنية، ١٩٩٤.

٣- المقالات والدوريات

١) د. أسامة محمد محى الدين عوض، جرائم الحاسب الآلي والجرائم الأخرى فى مجال تكنولوجيا المعلومات. بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائى، القاهرة ١٩٩٣.

٢) د. برهام محمد عطا الله، المصنفات المحمية فى قانون حماية حق المؤلف، منشور فى كتاب حق المؤلف بين الواقع والقانون، مركز البحوث والدراسات القانونية، كلية الحقوق جامعة القاهرة، ١٩٩٠.

٣) توفيق التوجيري، الفيس بوك والاتجاهات السلوكية، مجلة الصحة النفسية جامعة القاهرة، عدد ٨ ، ٢٠٠٩.

٤) زاهر راضي، استخدام مواقع التواصل الاجتماعي في العالم العربي، مجلة التربية، عدد ١٥ جامعة عمان الأهلية، عمان، ٢٠٠٣.

٥) نجوى عبد السلام فهمي، التفاعلية في المواقع الإخبارية على شبكة الإنترنت (Internet). دراسة تحليلية، المجلة المصرية لبحوث الرأي العام، العدد الرابع، القاهرة، ٢٠٠١.

٤- الندوات والمؤتمرات

١) د. زكى أمين حسونة، جرائم الحاسب الآلي والجرائم الأخرى فى مجال التكتيك المعلوماتى، بحث مقدم إلى المؤتمر السادس للجمعية المصرية للقانون الجنائى، القاهرة ١٩٩٣.

٢) علاء الدين محمد شحاته، رؤية أمنية للجرائم الناشئة عن استخدام الحاسب الإلى، بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة ١٩٩٣.

٣) د. محمد الأمين البشرى، التحقيق فى جرائم الحاسب الإلى، بحث مقدم إلى مؤتمر القانون والحاسب الآلي والإنترنت (Internet)، جامعة الإمارات العربية المتحدة،سنة ٢٠٠٠.

٤) د. هدى حامد قشقوش، جرائم الحاسب الآلي والجرائم الأخرى فى مجال تكنولوجيا المعلومات، - بحث مقدم للجمعية المصرية للقانون الجنائى ١٩٩٣

ثانيا: باللغة الانجليزية

1) Adams .L . Geverson , Media and society , Oxford publisher , London , 2006
2) Al-Mazeedi, Moosa, Ismail Ibrahim (1998). The Educational and Social Effect of the Internet on Kuwait University Students. In: Kuwait Conference on Information Highway. V:2 From : 16 – 18 March. P.p.
3) Al-Najran, Talal (1998). Internet adoption and use by Kuwait University students : new medium, same old gratifications. Unpublished Doctoral Dissertation. Ohio: The Ohio State University.
4) Bahgat Korany and others. The faces of national security in the Arab World, (England: Macmillan, 2009
5) Bajan, Peter, (1998). New Communities , New Social Norms. Studia-Psychologica. V. 40 (4.

6) Bartol, C. . Criminal behavior a psychosocial approach 5th, edition. New Jersey: Prentice Hall.2008
7) Bert Swart, "Modes of International Criminal Liability", in: Antonio Cassese, The Oxford Compaion to International Criminal Justice, Oxford University Press, 2009
8) Blackburn, R. . The psychology of criminal conduct: Theory, research and practice. Toronto:2006
9) Bolter, Jay David. Grusin Richard. (February 28, 2000), Remediation: Understanding New Media, USA: The MIT Press; 1st edition.
10)Brenner, V. (1997). Psychology of Computer Use: XL VII. Parameters of Internet Use, abuse and Addiction: The First 90 days of the Internet Usage Survey. Psychological Report, June, 80
11)Bright, J. "Community Safety, Crime Prevention and the Local Authority "in P. Willmott (ed) Poling and the Community, London PSL. 2008
12)Clinard, M. & Quinney, R. . Criminal behavior systems: A typology 6th, edition. Chicago: Pilgrimage.2007
13)Christakis, Nicholas A. Fowler, James H. (January 12, 2011), Connected: The Surprising Power of Our Social Networks and How They Shape Our Lives -How Your Friends' Friends' Friends Affect Everything You Feel, Think, and Do, USA: Back Bay Books; Reprint edition.
14)Cirel, P. Evans; McGillis, D. & Whit Comb, D. An Exemplary Project: Community Crime Prevention Programme, Seatte-Washington D.C.: Law Enforcement Assistance Administration, 2006
15)Daved smoloon (2009) the impact of the use of face book on the building society in the context of globalization, N Y sprctrum puplication.
16)Davis Lihmann, How can media improve our societies , George Publisher , New York , 2007
17)Diaz-Ortiz,Claire. (August 30, 2011), Twitter for Good: Change the World One Tweet at a Time, USA: Jossey-Bass; 1 edition.
18)Feldman, P. . The psychology of crime a social science textbook. Cambridge: Cambridge University Press.2006
19)Hawker, Mark. D, (August 25, 2010), Developer's Guide to Social Programming: Building Social Context Using Face book, Google Friend Connect, and the Twitter API, Canada: Addison-Wesley Professional; 1 edition.

20)Hollin, C. . Psychology and crime: An introduction to criminological psychology. New York: Routledge,2008
21)Hrdinová, J., Helbig, N., & Peters, C. S. (2010). Designing social media policy for government: Eight essential elements. Albany: Center for Technology in Government
22)Killy Nelson & Rinny Manwell , Media and crime , Media house , London , 2005
23)Kirkpatrick David,. (February 1, 2011), The Face book Effect: The Inside Story of the Company That Is Connecting the World. USA: Simon & Schuster.
24)Kraut, Robert et at (1998) . Internet Paradox : A Social Technology that Reduces Social Involvement and Psychological Well-Being . American Psychologist. V. 53, No. 9,.
25)Levinson, Paul. (September 5, 2009), New Media,USA: Allyn & Bacon;
26)Lister, Martin. Dovey, Jon. Giddings, Seth. Grant, Iain. Kelly, Kieran. (January 29, 2009) New Media: A Critical Introduction, USA/UK Europe : Routledge; 2 edition.
27)Nie, Norman and Erbing, Lutz (2017). Internet and Society: A Preliminary Report. Stanford Institute for the Quantitative Study of Society. Intersurvey Inc., and McKinsey and Co.
28)Prell, Christina. (November 9, 2011), Social Network Analysis: History, Theory and Methodology, USA/Austalia: Sage Publications Ltd.
29)Rowell, Rebecca. (January 2011), Youtube: The Company and Its Founders, UK Essential Library.
30)Sanders, CE; Field, TM.; Diego, M; and Kaplan (2000). The Relationship of Internet Use to Depression and Social Isolation among Adolescents. Adolescence. 35(138):
31)Schein, Levi, and Pollack, D, (1997). Social Work, Parenting and the Web. Journal of Family Social Work. 2(3): S/6.
32)Steward, Julian (1988). The Concept and Method of Cultural Ecology. In: High Points in Anthropology. Pual Bohannan and Mark Glazer (eds.). New York: McGraw-Hill, Inc.
33)Vonderau, Patrick. (December 30, 2009),The YouTube Reader, Sweden: National Library of Sweden.
34)White, H. et al. (1999) . Surfing the net in Later Life: A review of the Literature and Pilot Study of Computer use and Quality of life. Journal of Applied Gevontolog . Sept. V. 18 (3).

References:

1- alkutub

• d. 'abu alyazid ealaa almutyti, alhuquq ealaa almusanafat al'adabiat walfaniyat waleilmiati, munsha'at dar almaearifi, al'iiskandariati, altabeat al'uwlaa 1997.

• d. 'ahmad fathaa srur, alwasit faa qanun aleuqubati, alqism alkhasa, alqahirata, dar alnahdat alearabiati, 2010.

• aminat ealaa yusif, qarasinat 'anzimat alhasib alaly, almutamar alqawmaa althaalith eashar li'amn alhasib alali, , alqahirati, 1999

• antisar nuraa alghuribi, 'amn alhasib alali walqanunu0 dar alraatib alealamiat , lubnan,1994.

• da. jalal 'ahmad khalil, alnizam alqanunaa lihimayat alaikhtiraeat wanaql altiknulujia 'iilaa alduwal alnaamiati, jamieat alkuayt,1992.

• d. jamil eabd albaqaa alsaghir, alqanun aljanayia waltiknulujia alhadithatu, alkutaab al'awala, aljarayim alnaatijat ean aistikhdam alhasib al'iilaa , altabeat al'uwlaa, dar alnahdat alearabiati, 1992.

• hasan eimad mikawi, lilaa husayn, alaitisal wanazariaatuh almueasiratu, alqahirat, aldaar almisriat allubnaniatu, altabeat alraabieata, 'uktubar 2013

• salim khalid, thaqafat mawaqie altawasul aliajtimaeii walmujtamaeat almahaliyati, dar almutanabiy lilnashr waltawzie, qutru, 2005.

• shrif alliban , tiknulujia aliatisali. almakhatir waltahadiyat waltaathirat al'iijtimaeiati, alqahirati, alhayyat almisriat aleamat lilkitabi, 2008

• da. tariq surur, dhatiat jarayim al'iielam al'iilikturunii (dirasat muqaranati), alqahirata, dar alnahdat alnahdat alearabia .2001

• d. eabd alhamid aljamal, mabadi alqanun alkutaab althaanaa, alealaqat alqanuniatu, alfath liltibaeat walnashri, al'iiskandariati, 1990.

• d. eabd alrazaaq alsinhuraa, alwasit faa sharh alqanun almudanaa, alqahirat 1999.

• d. eabd aleazim mursaa waziru, sharh qanun aleuqubati- alqism alkhasa- jarayim alaietida' ealaa al'amwali, dar alnahdat alearabiat 1993.

• da.eabd alfataah alsayfaa, qanun aleuqubat allubnanaa - jarayim alaietida' ealaa 'amn aldawlat waealaa al'amwali, dar alnahdat alearabiati, bayrut 1972.
• d. eabd almuhaymin bakr, alqism alkhasu faa qanun aleuqubati, altabeat alsaabieat 1977.
• da0 eumar alsaeid ramadan, sharh qanun aleuqubati, alqism alkhasa, dar alnahdat alearabiat 1975.
• da. eumar alfaruq alhusaynaa, almushkilat aleamat faa jarayim alhasib al'iilaa wa'abeadiha alduwaliati, dirasatan tahliliatan naqdiatan binusus altashrie almisrii muqaranan bialtashrie alfaransaa , altabeat althaaniatu,1994.
• da. eawad muhamad, jarayim al'ashkhas wal'amwali, dar almatbueat aljamieiati, al'iiskandiriati.
• da. ghanim muhamad ghanim, eadam mulayimat alqawaeid altaqlidiat faa qanun aleuqubat limukafahat jarayim alhasib alali, mutamar alqanun walhasib alali wal'iintirnit (Internet)- al'iimarat, mayu 2000.
• fathi husayn eamir, wasayil alaitisal alhadithat min aljaridat 'iilaa alfis buk, alqahirati, alearabii lilnashr waltawziei, 2011
• du. fawziat eabd alsatar, sharh qanun aleuqubati, alqism alkhasa, dar alnahdat alearabiati,1983.
• da. majid eamar, almasyuwliat alqanuniat alnaashiat ean astikhdam fayrus baramij alhasib alali wawasayil himayitiha, dar alnahdat alearabiati, 2009
• d. muhamad husam litafaa, alhimayat alqanuniat libaramij alhasib alali, dar althaqafat liltibaeat walnashri. alqahirat 1987.
• da.muhamad samaa alshawaa, thawrat almaelumat waineikasatiha ealaa qanun aleuqubati, alqahirata, dar alnahdat alearabiati, altabeat althaaniat 2015.
• d. muhamad fahmaa talabah wakhrin, alhasibat alalkutruniat hadiraha wamustaqbalaha, mawsueatan dilta lilkumbiutir, matabie alkitaab almusraa alhadith 1992.
• d. muhamad mahyaa aldiyn eawad, alqanun aljanayia, jarayimuh alkhasat 1978/1979.
• d. muhamad mukhtar biribraa, qanun almueamalat altijariati, dar alfikr aleurbaa, sanat 1987.

• du.mahmud mahmud mustafaa, alqism alkhasi, dar alnahdat alearabiati, altabeat althaaminat 1984.
• d. mahmud mustafaa alqallaa, sharah qanun aleuqubat faa jarayim al'amwali, altabeat al'uwlaa,1939.
• d. mahmud najib husnaa, jarayim alaietida' ealaa al'amwal faa qanun aleuqubat allubnanaa, dar alnahdat alearabiati, bayrut
• , sharh qanun aleuqubati, alqism alkhasi, dar alnahdat alearabiati, 1988.
• mustafaa aljamali, mabadi alqanuni, alkutaab althaanaa, alealaqat alqanuniatu, alfath liltibaeat walnashri, al'iiskandiriati,1990.
• mishal 'iinula, tiqniaat aitisal hadithati: alwasayit almutaeadidat watatbiqatiha fi al'iielam walthaqafat waltarbiati, tarjamatu: nasr aldiyn aleiadi warabih alsaadiq, baris, dar alkitaab aljamieii, 2004.
• d. nabil 'iibrahim saeda, almadkhal 'iilaa alqanun alkutaab althaanaa, nazariat alhaq, dar alnahdat alearabiati, bayrut 1995.
• neum tshumiski, alsaytarat ealaa al'iielami.. al'iinjazat alhayilat lilburubajinda, taeriba: 'umimat eabd allatif, alqahirat, maktabat alshuruq alduwliati, altabeat althaaniatu, 2005
• da.hani duydar, nitaq ahtikar almaerifat altiknulujiat biwasitat alsiriyati, dar aljamieat aljadidati,1996.
• d. hudaa hamid qashqush, jarayim alhasib alalkutrunii faa altashrie almuqarini,alqahrata, dar alnahdat alearabiat 1992.
• d. hisham muhamad farid rustum, qanun aleuqubat wamakhatir tiqniat almaelumati, maktabat alalat alhadithat 'asyut 1994.
• d. halali eabd allaah 'ahmadu, taftish nuzam alhasib alali wadamanat almutaham almaelumati, alqahirata, dar alnahdat alearabiati.2006

2- alrasayil aleilmia

• da. khalid hamdi eabd alrahman, alhimayat alqanuniat lilkianat almantiqiati, risalat dukturatin, huquq eayn shams 1992.
• da. eazat mahmud 'ahmad khalil, mushkilat almasyuwliat almadaniat faa muajahat fayrus alhasibi. risalat dukturati, jamieat alqahirati, kuliyat alhuquqi, 1994.
• eimad 'iibrahim, 'athar aistikhdam alfis buk ealaa suluk talabat aljamieati, risalat majistir ghayr manshurtin, kuliyat altarbiati, jamieat eayn shams alqahirati, 2009.

• d. muhamad muhamad einb, mueayanat masrah aljarimati, risalat dukturat, 'akadimiat alshurtat, kuliyat aldirasat aleulya alqahirat 1988.
• di. yunis khalid earab mustafaa, jarayim alhasib alali (Computer) dirasat muqaranati, risalat majistir, aljamieat al'urduniyata, 1994.

3- almaqalat waldawriaat

• du. 'usamat muhamad mahaa aldiyn eawad, jarayim alhasib alali waljarayim al'ukhraa faa majal tiknulujia almaelumati. bahath muqadim lilmutamar alsaadis liljameiat almisriat lilqanun aljanayia, alqahirat 1993.
• d. birham muhamad eata allah, almusanafat almahmiat faa qanun himayat haqi almualafi, manshur faa kitab haqi almualaf bayn alwaqie walqanuni, markaz albuhuth waldirasat alqanuniati, kuliyat alhuquq jamieat alqahirati, 1990.
• tufiq altawjiri, alfis buk waliatijahat alsulukiatu, majalat alsihat alnafsiat jamieat alqahirati, eadad 8 , 2009.
• zahir rady, aistikhdam mawaqie altawasul alaijtimaeii fi alealam alearabii, majalat altarbiati, eadad 15 jamieat eamaan al'ahliati, eaman, 2003.
• najwaa eabd alsalam fahmi, altafaeuliat fi almawaqie al'iikhbariat ealaa shabakat al'iintirnit (Internet). dirasat tahliliati, almajalat almisriat libuhuth alraay aleami, aleadad alraabieu, alqahirata, 2001.

4- alnadawat walmutamarat

• d. zakaa 'amin hasuwnat, jarayim alhasib alali waljarayim al'ukhraa faa majal altaktik almaelumataa, bahath muqadam 'iilaa almutamar alsaadis liljameiat almisriat lilqanun aljanayia, alqahirat 1993.
• eala' aldiyn muhamad shahatuhu, ruyat 'amniat liljarayim alnaashiat ean aistikhdam alhasib al'iilaa, bahath muqadim lilmutamar alsaadis liljameiat almisriat lilqanun aljinayiy, alqahirat 1993.
• d. muhamad al'amin albushraa, altahqiq faa jarayim alhasib al'iilaa, bahath muqadam 'iilaa mutamar alqanun walhasib alali wal'iintirnit (Internet), jamieat al'iimarat alearabiat almutahidati,sanatan 2000.

• d. hudaa hamid qashqush, jarayim alhasib alali waljarayim al'ukhraa faa majal tiknulujia almaelumati, - bahth muqadim liljameiat almisriat lilqanun aljanayaa 1993

فهـــرس الموضوعـــات

الموضـــــوع الصفحة