مجلة جامعة دمشق للعلوم القانونية

مجلة جامعة دمشق للعلوم القانونية
المجلد 3 (3) – 2023 :

Damascus University Journal of Legal Sciences
Vol 3 (3)- 2023:

ذاتية الجرائم المعلوماتية في القانون السوري بالمقارنة مع قانون الجرائم المعلوماتية الأوربي "اتفاقية بودابست"

د. حسام الدّين ساريج[1]

1. مدرس في قسم القانون الجزائي – كلية الحقوق – جامعة دمشق

تاريخ الايداع : 2023/3/19
تاريخ القبول: 2023/6/8

الملخص:

يناقش البحث إشكالية دقيقة جداً هي ذاتية الجرم المعلوماتي من حيث الحق المعتدى عليه، ومن حيث عناصر الجرم وتحديدا العنصر المعنوي والعنصر المادي وذلك ضمن مقاربة تحليلية تأصيلية تتناول قانون الجرائم المعلوماتية السوري رقم 20 لعام 2022 ،وقانون جرائم تقنية المعلومات المصري لعام 2018 ،بالمقارنة مع قانون الجرائم المعلوماتية الأوربي أو اتفاقية بودابست لعام 2001 ،وقانون العقوبات الألماني، وقانون العقوبات الفرنسي، إلى جانب التشريعين الانجليزي والأمريكي.

وفد بدأ البحث بتحديد ذاتية الحق المعتدي، وذلك في المبحث الأول، حيث تم تناول هذه الذاتية في قانون الجرائم المعلوماتية الأوربي، وفي القانون السوري والقوانين المقارنة.

وفي المبحث الثاني تمت معالجة عنصري الجرم المعلوماتي المادي والمعنوي في ضوء قانون الجرائم المعلوماتي الأوربي والقانون السوري والقوانين المقارنة.

الكلمات المفتاحية: ذاتية الجرائم المعلوماتية ،اتفاقية بودابست، قانون الجرائم الأوربي.

Cybercrimes autonomy in Syrian law, comparison with European cybercrimes law "Budapest convention"

Dr. Hossam El-Din Sarij [1]

1. Lecturer in the Department of Criminal Law - Faculty of Law - Damascus University

Abstract:

The research discusses so accurate question is cybercrimes autonomy On the part of legal protected right, and cybercrime elements, specially criminal act and moral element, by analytic founding comparison with Syrian cybercrimes law number 20 date 17\3\2022, and Egyptian cybercrime law number 175 date 14\8\2018, and Budapest convention 2001, and German penal law, French penal code, and USA code, English statute.

The research divided into two chapters, the first treats autonomy of legal protected right as portrayed by Budapest convention 2001, Syrian law, and compared rules, the second focuses on material and moral element in light of Budapest convention 2001, Syrian law, and compared rules.

Kay words: Cybercrimes Autonomy, Budapest Convention, European Cybercrimes Law

Received: 19/3/2023
Accepted: 8/6/2023

المقدمة:

صدر قانون رقم 20 تاريخ 2022/4/18 المتضمن الجريمة المعلوماتية بمختلف صورها، وقد ألغى هذا القانون المرسوم التشريعي رقم 17 تاريخ 2012/2/8 الذي أعلنت المادة الأولى منه أنه يتضمن "قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية".

وقد بدأ هذا القانون بجملة واسعة من التعريفات حيث عرّف الدولة والهيئة الوطنية والهيئة الناظمة والمعلومات ووسائل تقانة المعلومات والبرمجيات ونظام المعلومات والشبكة والموقع الالكتروني وعنوانه والتطبيق و معلومات الجهة العامة والتواصل على الشبكة والمحتوى الرقمي والحساب الشخصي ومقدم الخدمة على الشبكة ومقدم خدمات النفاذ إلى الشبكة ومقدم خدمات الاستضافة ومقدم خدمات التطبيقات على الشبكة والبرمجيات الخبيثة واسم الموقع الالكتروني ونطاق على الانترنت واسم النطاق العلوي واسم النطاق العلوي الوطني واسم النطاق العلوي السوري والجريمة المعلوماتية والدليل الرقمي و بيانات الحركة والخصوصية والترخيص النمطي وأخيراً البطاقة الالكترونية.

وعلى الرغم من عدم وجود ترتيب منطقي لهذا العدد من هذه التعريفات فمثلاً بعد تعريف البرنامج جاء تعريف التطبيق بعده بعدة تعريفات ثم بعده بعدة تعريفات جاء تعريف البرمجيات الخبيثة مع أن المنطق أن يأتي تعريف التطبيق والبرمجيات الخبيثة بعد تعريف البرنامج مباشرة، قد تراوحت هذه التعريفات بين التقني والبديهي، فمثلاً من البديهيات في يومنا هذا أو في القرن الواحد والعشرين تعريف البطاقة الالكترونية أو الدولة أو البرنامج أو التطبيق أو الشبكة أو البرمجيات الخبيثة أو التواصل على الشبكة أو الموقع أو عنوان الموقع.

وقد جاء هذا القانون بتعريف للجرم المعلوماتي بأنه

سلوك مجرَّم وفقاً لأحكام هذا القانون يقترف بواسطة وسائل تقانة المعلومات، يستهدف المعلومات أو نظم المعلومات أو يرتبط بإضافة محتوى رقمي على الشبكة.

وكان المرسوم التشريعي رقم 17 لعام 2012 المتضمن قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية قد عرّف الجرم المعلوماتي بأنه:

جريمة ترتكب استخدام الأجهزة الحاسوبية أو الشبكة أو تقع على المنظومات المعلوماتية أو الشبكة.

وواضح للعيان حجم الاختلاف والتباين بين التعريفين، فالتعريف الجديد يركز على المحل والحق المعتدى عليه، بينما التعريف القديم أوسع من التعريف الجديد لأنه يعد الجرم جرماً معلوماتياً أذا كان محله بيانات الحاسوب أو إذا كان الحق المعتدى عليه بيانات الحاسوب.

وقد وقع القانون الجديد في فخ التناقض لأنه تضمن جرائم عدها بصريح النص جرائم معلوماتية لأنها وردت في الفصل الرابع منه المعنون بالجرائم المعلوماتية، مع أنها في الواقع ليست جرائم معلوماتية وفقاً لتعريف الجرم المعلوماتي لأن محلها بيانات الحاسوب كجريمة الذم الالكتروني، فهذه الجريمة تقع (كما هو ثابت) على الاعتبار كحق أو قيمة ولا تستهدف إطلاقاً بيانات الحاسوب.

وقد أضاف القانون الجديد عبارة مضللة لتعريف الجرم المعلوماتي هي" أو يرتبط بإضافة محتوى رقمي على الشبكة" وهذه العبارة مضللة لأنها تكرار بمفردات مغايرة لعبارة "يقترف بواسطة وسائل تقانة المعلومات" فالثابت أن إضافة محتوى رقمي يعني استخدام وسائل تقانة المعلومات فكيف نتصور وجود المحتوى دون استخدام وسائل تقانة المعلومات.

وبالمقارنة مع قانون الجرائم المعلوماتية الأوربي أو اتفاقية بودابست[1]تاريخ 2001/11/23 نجد أنها احتوت فقط على التعريفات التقنية الأربعة :

1. نظام حاسوبي[2]
2. بيانات حاسوبية[3]
3. خادم أو مزود الخدمة[4]
4. بيان الحركة[5]

إشكالية البحث:

الإشكالية الرئيسية تنطلق من عنوان البحث وهي ذاتية الجرائم المعلوماتية التي تناولها القانون رقم 20 لعام 2022 وذلك من خلال مقارنتها مع الجرائم المعلوماتية، التي احتواها قانون الجرائم المعلوماتية الأوربي أو ما بات يعرف باتفاقية بودابست لعام 2001[6].

ويتفرع من هذه الإشكالية إشكاليات فرعية:

1. ذاتية الحق المعتدى عليه أو المصلحة المحمية وبعبارة أدق هل هناك خلط بين المحل أي بيانات الحاسوب وبيانات الحاسوب باعتبارها الحق المعتدى عليه.
2. ذاتية عنصري الجريمة المادي والمعنوي

---

[1]وقعت الدول الأوربية برتوكولاً مضافاً للاتفاقية يتضمن تجريم العنصرية وكراهية الأجانب المرتكبة من خلال نظام معلوماتي، وذلك في 2003/1/28 .

[2]Computer system
any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data

[3]Computer data
any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function

[4]Service provider
any public or private entity that provides to users of its service the ability to communicate by means of a computer system, andany other entity that processes or stores computer data on behalf of such communication service or users of such service

[5] traffic data
any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.

[6]تضمنت الاتفاقية أربعة فصول:
1- المصطلحات
2- التدابير الموضوعية والشكلية
3- التعاون الدولي
4- الأحكام الختامية

أهداف البحث:

يهدف البحث إلى الوقوف على ذاتية ما يسمى بالجرم المعلوماتي كما جرمه القانون السوري وبعبارة أدق هل هناك جرم معلوماتي، بدءاً من الحق المعتدى عليه ثم عناصر الجريمة .

حيث سنحدد الحق المعتدى عليه في مختلف الجرائم المعلوماتية بدءاً من أهمها وهي جريمة الاختراق أو الدخول غير المشروع كما عنونها القانون السوري أو الوصول غير القانوني كما عنونها قانون الجرائم المعلوماتية الأوربي،

إلى جانب هذه الجريمة، هناك جرائم أخرى لا تقل أهمية هي جرائم التأثير على البيانات، التأثير على النظام، اعتراض البيانات، تصميم وتوفير وسائل ارتكاب الجرائم المعلوماتية من برامج وكلمات مرور وما سواها، فضلاً عن الاحتيال المعلوماتي والتزوير المعلوماتي وإساءة الائتمان المعلوماتي.

وتحديد الحق المعتدى عليه من الأهمية بمكان، خصوصاً أن هناك بعض هذه الجرائم، مجرم بالفعل باعتباره جرماً عادياً، كالاحتيال وإساءة الائتمان والتزوير والإتلاف،

إلى جانب الحق المعتدى عليه وما يعتريه من ذاتية، ينطلق البحث باتجاه تحديد ذاتية عنصري الجريمة المعنوي والمادي، على ضوء القانون السوري، فضلاً عن القانون الأوربي إلى جانب قانون العقوبات الفرنسي وقانون العقوبات الألماني والتشريع الانجليزي والتشريع الأمريكي، ومن التشريعات العربية سندرس الذاتية على ضوء قانون حديث نسبياً هو قانون مكافحة جرائم تقنية المعلومات المصري رقم 148 لعام 2018 وهو من أحدث تشريعات مكافحة الجريمة المعلوماتية على الصعيد العربي،ويمثل تطوراً هاماً في سياق التجريم المعلوماتي.

أهمية البحث:

في عالم افتراضي يتوسع يومياً عالم يوازي في وجوده العالم الحقيقي عالم من مواقع الويب والمدونات و الايميل أو البريد الرقمي عبر الشابكة ومواقع التواصل الاجتماعي ومحركات البحث والمنتديات وصفحات التواصل والتجارة أو الاقتصاد الرقمي.

من هنا يناقش البحث موضوعاً هاماً وحديثاً حيث لا يشكك أحد في حجم وخطورة الإجرام المعلوماتي أما حداثة الموضوع فتتبع من حداثة القانون السوري فلم يمض أشهر على صدوره ما يستدعي بالضرورة تحليل ذاتية الجرائم المعلوماتية الواردة فيه ومما يزيد الأمر وضوحاً ودقة هو المقارنة التفصيلية لما هو مجرم في عدد من التشريعات الأجنبية كقانون العقوبات الفرنسي وقانون العقوبات الألماني فضلاً عن التشريعين الانجليزي والأمريكي.

كما تنبع أهمية البحث من محاولة الباحث تقديم تصور حقيقي لمفهوم كل جريمة من جرائم المعلوماتية خصوصاً على ضوء التقارب والاختلاف في تحديد النموذج القانوني لكل جريمة من هذه الجرائم.

فهذا البحث يقدم مقاربة وإضاءة قانونية فقهية وإلى حد ما قضائية للفلسفة التي تقف وراء القوانين والتشريعات محل الدراسة وخصوصاً القانون الأوربي للجرائم المعلوماتية والقانون السوري رقم 20 لعام 2022 الخاص بالجريمة المعلوماتية.

منهج البحث:

سنتبع في تناول موضوعات البحث المنهج التحليلي فضلاً عن المنهج التأصيلي حيث سنحلل النصوص الجزائية في قانون الجرائم المعلوماتية السوري رقم 20 لعام 2022 وقانون الجرائم المعلوماتية الأوربي كما سنتبع المنهج المقارن من خلال دراسة النظام اللاتيني أو ما بات يسمى بنظام القانون المدني Civil law،وكنموذج عليه سندرس الجرائم المعلوماتية في قانون العقوبات الفرنسي وقانون العقوبات الألماني كما سندرس النظام الإنجليزي وأمريكي أو ما يسمى بنظام القانون العرفي Common law وكنموذج عليه سندرس التشريعين الانجليزي والأمريكي.

وسنقسم البحث إلى مبحثين وذلك على النحو الآتي:

المبحث الأول: ذاتية الحق المعتدى عليه

المطلب الأول: في قانون الجرائم المعلوماتية الأوربي

المطلب الثاني: في القانون المقارن والقانون السوري

المبحث الثاني: ذاتية عناصر الجرم المعلوماتي

المطلب الأول: في قانون الجرائم المعلوماتية الأوربي

المطلب الثاني: في القانون المقارن والقانون السوري

المبحث الأول

ذاتية الحق المعتدى

سندرس في هذا المبحث أولاً الذاتية في قانون الجرائم المعلوماتية الأوربي وذلك في المطلب الأول ثم ننتقل لمعالجة ذاتية الحق المعتدى عليه في القانون المقارن والقانون السوري وذلك في المطلب الثاني.

المطلب الأول:

في قانون الجرائم المعلوماتية الأوربي

حدد قانون الجرائم المعلوماتية الأوربي في مقدمة اتفاقية بودابست القيمة أو الحق المعتدى عليه بنظم الحاسوب أو الكمبيوتر والشيكات و البيانات وتحديداً سرية وسلامة وتوافر نظم الحاسوب أو الكمبيوتر والشبكات والبيانات.

كما أكدت الاتفاقية على الحق في التعبير دون أي تدخل وأكدت أيضاً على الحق في حرية التعبير وما يتفرع عنه من الحق في حرية البحث وتلقي ونقل المعلومات والأفكار كما أكدت على الحق في احترام الخصوصية والحق في حماية البيانات الشخصية فضلاً عن احترام وحماية حقوق الطفل أو حقوق القصر إلى جانب حماية الاعتبار وحماية حقوق النشر والتأليف والحقوق المجاورة.

وبعد هذا التحديد العام للحق المعتدى عليه جاءت اتفاقية بودابست لتحدد بدقة الحق المعتدى عليه بسرية وسلامة وتوافر البيانات والأنظمة[7] وذلك في جرائم الفضاء الالكتروني[8] وهي جرائم الاختراق أو الوصول غير القانوني[9] والاعتراض غير القانوني[10] والتدخل أو التأثير أو التلاعب بالبيانات[11] و التدخل أو التأثير أو التلاعب بالأنظمة[12] وأخيراً جريمة التعامل بأدوات التأثير على البيانات أو الأنظمة ويشمل التعامل صناعة أو توزيع أو استيراد أو حيازة أدوات تستخدم في ارتكاب الجرائم المعلوماتية المذكورة كالبرامج وكلمات دخول أو مرور[13].

وقد ميزت الاتفاقية بوضوح بين جرائم الفضاء الالكتروني من جهة والجرائم التقليدية التي ترتكب من خلال الانترنت أو الشبكة من جهة أخرى، والتي من شأنها انتهاك حقوق المؤلف أو الاعتداء على الاعتبار أو الاعتداء على حقوق الأطفال وقد تتضمن تعاملات مالية غير قانونية أو تتضمن عرض خدمات غير قانونية.

وبالتالي وفقاً لاتفاقية بودابست لا تعد جرائم معلوماتية الجرائم التقليدية الآتية:

1. الاحتيال المرتبط بالكمبيوتر[14]
2. التزوير المرتبط بالكمبيوتر[15]
3. استغلال الأطفال في المواد الإباحية[16]
4. انتهاك حقوق التأليف والنشر[17]

هذه الجرائم عالجتها الاتفاقية أو رأى معدو الاتفاقية أن تتناولها الاتفاقية لارتكابها باستخدام الانترنت أو الشبكة وليس لأنها جرائم معلوماتية.

وهناك جرائم أخرى تمت مناقشتها لكنها لم تدرج ضمن الاتفاقية وخصوصاً ما يرتكبه شاغلو أو محتلو الفضاء الالكتروني[18]من إدراج نطاق مطابق لنطاق تجاري حقيقي معروف بقصد ابتزاز مالكي النطاق التجاري الحقيقي وقد رأى واضعو الاتفاقية عدم تضمين هذا الفعل ضمن الاتفاقية باعتبار أن الحق المعتدى عليه هو العلامة التجارية[19].

المطلب الثاني:

في القانون المقارن والقانون السوري

تردد لمشرعون في تحديد الحق المعتدى عليه وبعبارة أدق هناك فوضى تشريعية في تحديد هذا الحق فنجد المشرع الفرنسي وضع الجرائم المعلوماتية في الكتاب الثالث من قانون العقوبات الفرنسي في الباب الثاني في الفصل الثالث منه تحت عنوان " الوصول غير المسموح لأنظمة المعالجة الآلية للبيانات[20]".

---

[7] Confidentiality, Integrity and Availability of computer data and systems
[8] Cyber-space offences
[9] Illegal access
[10] Illegal interception
[11] Data interference
[12] System interference
[13] Misuse of devices
[14] Computer-related fraud
[15] Computer-related forgery
[16] Unlawful production or distribution of child pornography by use of computer systems
[17] Offences related to infringements of copyright and related rights
[18] Cyber-squatters
[19] Explanatory Report page 10

وقد عدّ المشرع الفرنسي البيانات مال وهذا التحديد لطبيعة البيانات مستفاد من وضع المشرع الفرنسي الجرائم المعلوماتية في الكتاب الثالث من العقوبات المتعلق بالجرائم والجنح الماسة بالملكية[21]وذلك إلى جانب السرقة والاحتيال وإساءة الائتمان والإتلاف وغسل الأموال.

وبذلك يكون المشرع الفرنسي قد عدّ النظام وليس البيانات هو الحق المعتدى عليه في الجرائم المعلوماتية لكنه في الوقت ذاته وضع الجرائم المعلوماتية ضمن جرائم الأموال وهذا يعني أن الحق المعتدى عليه هو المال المعلوماتي أو البيانات وليس نظام معالجة البيانات ومن هناك نستنتج تناقض خطة المشرع الفرنسي فالحق المعتدى عليه يتراوح بين نظام المعالجة الآلية وبين البيانات.

والجدير بالوقوف هو أن المشرع الفرنسي عدّ إضعاف الثقة العامة[22] هي المصلحة المحمية سواء أكان ذلك في جريمة التزوير المعلوماتي أي التزوير في محرر معلوماتي[23] معد للإثبات أو التزوير التقليدي أي التزوير في محرر ورقي [24] معد للإثبات وفي الوقت ذاته عد تدمير محرر معلوماتي وصفاً مشدداً لجرم الوصول غير المسموح لمنظومة معلوماتية[25].

وإذا اتجهنا إلى الخطة الألمانية في معالجة الحق المعتدى عليه نجد دقة أكبر في تحديد المصلحة المحمية وهذا ليس غريباً على العقيدة الجنائية الألمانية التي تتمحور حول التحديد الدقيق للمصلحة المحمية[26] في كل جريمة بدقة بالغة.

ففي قانون العقوبات الألماني وردت جرائم معلوماتية في المواد 303أ و303ب و202 أ و202 ب و202 ج 263 أ و 269 و 270 وهي تقريباً كلها مواد مكررة عد مادتي التزوير269المادة و الخداع المادة 270 :

1. التأثير بنوعيه :

. على البيانات[27] في المادة 303 أ من قانون العقوبات الألماني

. على النظام[28]في المادة 303 ب من قانون العقوبات الألماني

---

[20]UNAUTHORISED ACCESS TO AUTOMATED DATA PROCESSING SYSTEMS

[21]FELONIES AND MISDEMEANOURS AGAINST PROPERTY

[22]UNDERMINING PUBLIC TRUST

[23]medium of expression

[24]ARTICLE 441-1:

Forgery consists of any fraudulent alteration of the truth liable to cause harm and made by any means in a document or other **medium of expression of which** the object is, or effect may be, to provide evidence of a right or of a situation carrying legal consequences. Forgery and the use of forgeries is punished by three years' imprisonment and a fine of € 45,000.

[25]د. علي عبد القادر قهوجي الحماية الجنائية للبيانات المعالجة الكترونياً بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنت المنعقد في جامعة الإمارات العربية المتحدة ـ كلية الشريعة والقانون ـ مايو 2000 بحوث المؤتمر المجلد الثاني الطبعة الثالثة 2004 ص591

د. أشرف توفيق شمس الدين الحماية الجنائية للمستند الالكتروني دراسة مقارنة الطبعة الأولى دار النهضة العربية 2006ص15

[26]Rechtsgut

[27]Artikel 303a

Datenveränderung

(1) WerrechtswidrigDaten (§ 202a Abs. 2) löscht, unterdrückt, unbrauchbarmachtoderverändert, wirdmitFreiheitsstrafebiszuzweiJahrenodermitGeldstrafebestraft.

(2) Der Versuchiststrafbar.

عطفت المادة 303 أ على المادة 202 بفقرتها الثانية في تعريفها للبيانات فلم تحدد هذه الفقرة ما إذا كانت البيانات هي أشياء أو أموال،وإنما عرفتها بأنها تلك المخزنة أو المنقولة كهربائياً أو مغناطيسياً وغير الملموسة.

[28]Artikel 303b

Computersabotage

(1) WereineDatenverarbeitung, die füreinenfremdenBetrieb, einfremdesUnternehmenodereineBehörde von wesentlicherBedeutungist, dadurchstört, daßer

2. الحصول على البيانات[29] المادة 202 أ والاعتراض المادة 202 ب والتعامل بأدوات القرصنة 202 ج من فانون العقوبات الألماني.

3. الاحتيال[30] الحاسوبي المادة 263 أ من قانون العقوبات الألماني

4. التزوير[31] بأنواعه[32] المواد 268[33]. 269 .270 من قانون العقوبات الألماني.

---

1. eine Tat nach § 303a Abs. 1 begehtoder
2. eineDatenverarbeitungsanlageodereinenDatenträgerzerstört, beschädigt, unbrauchbarmacht, beseitigtoderverändert,
wirdmitFreiheitsstrafebiszufünfJahrenodermitGeldstrafebestraft.
(2) Der Versuchiststrafbar.

[29]Artikel 202a
Ausspähen von Daten
(1) WerunbefugtDaten, die nichtfürihnbestimmt und die gegenunberechtigten Zugangbesondersgesichertsind, sichodereinemanderenverschafft, wirdmit FreiheitsstrafebiszudreiJahrenodermitGeldstrafebestraft.
(2) DatenimSinne des Absatzes 1 sindnursolche, die elektronisch, magnetischoder sonstnichtunmittelbarwahrnehmbargespeichertsindoderübermitteltwerden.

[30]Artikel 263a
Computerbetrug
(1) Wer in der Absicht, sichodereinemDritteneinenrechtswidrigenVermögensvorteilzuverschaffen, das Vermögeneinesanderendadurchbeschädigt, daßer das ErgebniseinesDatenverarbeitungsvorgangsdurchunrichtigeGestaltung des Programms, durchVerwendungunrichtigeroderunvollständigerDaten, durchunbefugteVerwendung vonDatenodersonstdurchunbefugteEinwirkung auf den Ablaufbeeinflußt, wirdmitFreiheitsstrafebiszufünfJahrenodermitGeldstrafebestraft.
(2) § 263 Abs. 2 bis 7 gilt entsprechend.
(3) WereineStraftatnachAbsatz 1 vorbereitet, indemerComputerprogramme, derenZweck die Begehungeinersolchen Tat ist, herstellt, sichodereinemanderen
verschafft, feilhält, verwahrtodereinemanderenüberlässt, wirdmitFreiheitsstrafe biszudreiJahrenodermitGeldstrafebestraft.
(4) In den Fällen des Absatzes 3 gilt § 149 Abs. 2 und 3 entsprechend.

[31]Artikel 268
FälschungtechnischerAufzeichnungen
(1) WerzurTäuschungimRechtsverkehr
1. eineunechtetechnischeAufzeichnungherstelltodereinetechnische Aufzeichnungverfälschtoder
2. eineunechteoderverfälschtetechnischeAufzeichnunggebraucht,
wirdmitFreiheitsstrafebiszufünfJahrenodermitGeldstrafebestraft.
(2) TechnischeAufzeichnungisteineDarstellung von Daten, Meß- oderRechenwerten,ZuständenoderGeschehensabläufen, die durcheintechnischesGerätganzoderzumTeilselbsttätigbewirktwird, den Gegenstand der Aufzeichnungallgemeinoderfür Eingeweihteerkennenläßt und zumBeweiseinerrechtlicherheblichenTatsachebestimmtist, gleichvielobihr die Bestimmungschonbei der Herstellungodererstspätergegebenwird.
(3) Der Herstellungeinerunechtentechnischen Aufzeichnungstehtesgleich, wenn derTäterdurchstörendeEinwirkung auf den Aufzeichnungsvorgang das Ergebnis der Aufzeichnungbeeinflußt.
(4) Der Versuchiststrafbar.
(5) § 267 Abs. 3 und 4 gilt entsprechend.

Artikel 269
FälschungbeweiserheblicherDaten

والملاحظ أن المادة 268 من قانون العقوبات الألماني جرّمت إنتاج مستند تفني مزور أو تزوير مستند تقني وهذا المستند يحتوي بيانات قياسات أو حسابات أوصاف أو تسلسل أحداث وهذا المستند معد باعتباره دليلاً في الإثبات أما المادة 269 جرّمت تزوير البيانات بالحفظ أو التغيير كما عدت المادة 270 تزوير البيانات أثناء معالجتها معادلاً للتزوير بعد المعالجة.

هذه الخطة الألمانية المتكاملة للجريمة المعلوماتية انطلقت من تحديد دقيق المصلحة المحمية ولو أردنا تسليط الضوء على المصلحة المحمية لوجدنا أنها تختلف باختلاف الجريمة المعلوماتية ففي جريمة التأثير على البيانات أو على المنظومة المعلوماتية نجد المشرع الألماني حدد المصلحة المحمية بالأشياء المملوكة للغير[34] لأنها وضعها في الباب السابع والعشرين من القسم الخاص وقد عنون هذا الباب بـ "إلحاق الضرر بالأشياء[35]" لكن جانب من الفقه يرى أن المصلحة الحمية تكمن أيضاً في حماية الاقتصاد عبر التشغيل السليم لعمليات معالجة البيانات[36]أما جرائم الحصول على البيانات والاعتراض والتعامل بأدوات القرصنة فقد وضعها المشرع الألماني في الباب الخامس عشر من القسم الخاص المعنون بـ الاعتداء على الحياة الخاصة والسرية أما جريمة الاحتيال الحاسوبي فقد جاءت بعد جريمة الاحتيال التقليدي وفي ذات الباب أي في الباب الثاني والعشرين من القسم الخاص الذي تناول الاحتيال وخرق الثقة[37]،وبذلك لم يجد المشرع فارقاً بين الجريمتين أي الاحتيال بنوعيه التقليدي والحاسوبي والثابت أن المصلحة المحمية في الاحتيال هي المال المملوك للغير.

أما التزوير المعلوماتي[38]ومن خلاله تحمى الثقة بالوثائق المعدة للإثبات فقد جاء في الباب الثالث والعشرين من القسم الخاص المتعلق بتزوير المستندات[39].

---

1) WerzurTäuschungimRechtsverkehrbeweiserheblicheDaten so speichertoder verändert, daßbeiihrerWahrnehmungeineunechteoderverfälschteUrkundevorliegen würde, oderderartgespeicherteoderveränderteDatengebraucht, wirdmit FreiheitsstrafebiszufünfJahrenodermitGeldstrafebestraft.
(2) Der Versuchiststrafbar.
(3) § 267 Abs. 3 und 4 gilt entsprechend.

[32]Artikel 270
TäuschungimRechtsverkehrbeiDatenverarbeitung
Der TäuschungimRechtsverkehrsteht die fälschlicheBeeinflussungeinerDatenverarbeitungimRechtsverkehrgleich.

[33]Georg KüpperStrafrechtBesondererTeillDeliktegegenRechtsgüter der Person und Gemeinschaft Springer-Verlag Berlin Heidelberg 1996 S.99

تتعلق هذه المادة بالتلاعب بجهاز تسجيل السرعة في السيارات وقبل سن هذه المادة خلص القضاء الألماني إلى أن التلاعب بهذا الجهاز لا يؤلف تزويراً باعتبار أن التزوير يقع على وثيقة.

[34]Wolfgang MitschStrafrechtBesondererTeil 2 Vermogensdelikte(Randbereich) Teilband 2Springer-Verlag 2001 S.432

[35]Sachbeschädigung

[36]Jan Vetter Gesetzeslückenbei der InternetkriminalitätStuttgart 2002 S.44

[37]Betrug und Untreue

[38]Georg KüpperStrafrechtBesondererTeillDeliktegegenRechtsgüter der Person und Gemeinschaft Springer-Verlag Berlin Heidelberg 1996 S.100

[39]Urkundenfälschung

ولو حللنا المصالح المحمية في الجرائم المعلوماتية لوجدنا أنها لا تختلف إطلاقاً عن الجرائم التقليدية المشابهة لها وبعبارة أدق نخلص إلى التأصيل الدقيق لخطة المشرع الألماني لنقول أن اختلاف محل الجريمة وهو البيانات لم يرتب أي اختلاف في المصلحة المحمية وبعبارة أكثر دقة تقوم خطة المشرع الألماني على التماهي بين الجرم المعلوماتي والجرم التقليدي وعدم التمييز بينهما.

وفي بريطانيا يعد قانون إساءة استخدام الحاسوب لعام 1990 (المعدل)الشرعة العظمى في مواجهة الجريمة المعلوماتية فالجريمة الأساسية فيه هي الدخول إلى منظومة أو الاختراق[40]وفضت محكمة الاستئناف بأنه قد يتم الاختراق مباشرة من خلال ذات الحاسوب المخترق أو يتم الاختراق من حاسوب أخر مختلف عن الحاسوب المخترق.

وفي قصية أخرى رأت المحكمة أن استخدام حاسوب العمل من قبل ضباط الشرطة لأغراض شخصية كتصفح الإيميل لا يؤلف جريمة الاختراق وفقاً لقانون إساءة استخدام الحاسوب باعتبار لديهم الحق بالدخول إلى حاسوب العمل.

وتمت إدانة عاملة (وقد صدق الإدانة مجلس اللوردات)في مصرف أمريكان أكسبريس بجرم الاختراق لأنها دخلت إلى 189 حساب لا يحق لها الدخول إليها[41].

كما جرَّم قانون تنظيم سلطات التحقيق لعام 2000 الاعتراض[42]وفي قضية تتلخص وقائعها بوضع الشرطة الإنجليزية جهاز تنصت سري في سيارة المدعى عليه يسجل الكلمات التي قالها المدعى عليه أثناء وجوده في السيارة بما في ذلك ما يقوله في أثناء محادثة عبر الهاتف

قضت محكمة الاستئناف أن المعنى الطبيعي لتعبير "اعتراض" يدل على بعض التداخل أو التجريد للإشارة، سواء كانت تمر عبر الأسلاك أو عن طريق التلغراف اللاسلكي، أثناء عملية الإرسال. وإن تسجيل صوت الشخص، بصرف النظر عن حقيقة أنه كان في الوقت الذي يستخدم فيه الهاتف، لا يؤلف اعتراضا.[43]

---

[40]Section 1(1)
provides that a person is guilty of an offense if:
a. he causes a computer to perform any function with intent to secure access
to any program or data held in any computer;
b. the access he intends to secure is unauthorized; and
c. he knows at the time when he causes the computer to perform the function that this is the case.
Subsection (2) provides that the intent a person has to have to commit an offence under this section need not be directed at:
a. any particular program or date;
b. a program or data of any particular kind; or
c. a program or data held in any particular computer.

[41]تمت معالجة هذا الموقف بشكل صريح من خلال قانون الاحتيال وإساءة استخدام الحاسوب الأمر يكذب استخدام عبارة "تم الوصول إلى حاسوب دون إذن أو تجاوز الوصول المصرح به.

[42]Unlawful interception
1. It shall be an offence for a person intentionally and without lawful authority to intercept, at any place in theUnited Kingdom, any communication in the course of it
transmission by means of … (b) a public telecommunication system.
2. It shall be an offence for a person (a) intentionally and without lawful authority … to intercept, at any place in the United Kingdom, any communication in the course
of its transmission by means of a private telecommunication system."

[43]Eoghan Casey Digital Evidence and Computer CrimeForensic Science, Computers and the Internet Third Edition p.139

كما جرّم قانون إساءة استخدام الكمبيوتر الانجليزي لعام 1990 التدخل في البيانات والتدخل في النظام [44]وبصورة خاصة عن طريق الفيروسات والديدان وأحصنة طروادة[45]ة كما أدخل قانون الشرطة والعدالة لعام 2006 تعديل على قانون إساءة استخدام الكمبيوتر ويتضمن هذا التعديل كافة صور التعامل بالبرمجيات المدمرة[46]كما يخضع التزوير المعلوماتي للمادة الثانية من قانون إساءة استخدام الكمبيوتر التي جرّمت الوصول غير المسموح بقصد ارتكاب جريمة أخرى أما الاحتيال المعلوماتي فهو مجرم بموجب الفقرة الخامسة من المادة الثانية من قانون الاحتيال حيث عدت هذه الفقرة الادعاء أو التصوير الكاذب متحققاً إذا اتخذ شكل التلاعب بنظام حاسوبي.[47]

---

[44]section 3 of the English Computer Misuse Act 1990, as amended,
1. A person is guilty of an offence if—
a. he does any unauthorized act in relation to a computer;
b. at the time when he does the act he knows that it is unauthorized; and
c. either subsection (2) or subsection (3) applies.
2. This subsection applies if the person intends by doing the act—
a. to impair the operation of any computer;
b. to prevent or hinder access to any program or data held in any computer; or
c. to impair the operation of any such program or the reliability of any such data.
3. This subsection applies if the person is reckless as to whether the act will do any of the things mentioned in paragraphs (a) to (c) of subsection (2) above.

[45]Worms and computer viruses Trojans.

[46]the Police and Justice Act 2006 created a new set of offenses concerning the misuse of devices, inserting section 3A into the 1990 Act in the following terms:
1. A person is guilty of an offence if he makes, adapts, supplies, or offers to supply any article intending it to be used to commit, or to assist in the commission of, an offence under section 1 or 3.
2. A person is guilty of an offence if he supplies or offers to supply any article believing that it is likely to be used to commit, or to assist in the commission of, an offence under section 1 or 3.
3. A person is guilty of an offence if he obtains any article with a view to its being supplied for use to commit, or to assist in the commission of, an offence under section 1 or 3.
4. In this section "article" includes any program or data held in electronic form.

[47]The Fraud Act of 2006 updated the law in England. Section 2 sets out the offence of fraud by false representation:
1. 2.—(1) A person is in breach of this section [and thereby is guilty of fraud according to section 1] if he
a. dishonestly makes a false representation, and
b. intends, by making the representation—
i. to make a gain for himself or another, or
ii. to cause loss to another or to expose another to a risk of loss.
2. A representation is false if—
a. it is untrue or misleading, and
b. the person making it knows that it is, or might be, untrue or misleading.
3. "Representation" means any representation as to fact or law, including a

وبذلك يكون القانون الانجليزي قد سبق الاتفاقية الأوربية في تحديد المصلحة المحمية في الجريمة المعلوماتية "بيانات الحاسوب" بأبعادها الثلاثة السلامة والثقة والتوافر.

وإذا توجهنا إلى التشريع الأمريكي نجد القانون الاتحادي قد تناول العديد من جرائم المعلوماتية كالاحتيال والابتزاز وسرقة الهوية والاختراق كما تناول الملكية الفكرية والمحتوى الإباحي المتعلق بالأطفال[48].

وواضح من تحليل هذه المواد أن المصلحة المحمية في جرائم المعلوماتية هي بيانات الحاسوب و كما هو الحال في اتفاقية بودابست، جرم المشرع الأمريكي الاحتيال المرتبط بالحاسوب كما جرّم المحتوى الإباحي الماس بالأطفال فضلاً عن الأفعال الماسة بالملكية الفكرية.

والسؤال الآن هل حدد المشرع السوري الحق المعتدى في جرائم المعلوماتية التي تناولها القانون 20 لعام 2022 ؟

الجواب بالقطع بالنفي فقد وردت الجرائم المعلوماتية في الفصل الرابع من هذا القانون دون عنونة لهذا الفصل تشير إلى الحق المعتدى ثم ذكرت الجرائم المعلوماتية تباعاً في المواد(11 . 31) بعبارة أدق ذكرت الجرائم المعلوماتية دون حصرها بفئات وبالتالي لم تحدد الحقوق المعتدى عليها في هذه الفئات.

وبالمقارنة مع سياسة المشرع المصري في مقاربة الإجرام المعلوماتي نجد اهتمام المشرع المصري في تحديد الحق المعتدى عليه في قانون رقم 175 لعام 2018 في شأن جرائم مكافحة تقنية المعلومات ففي الباب الثالث من هذا القانون جاء الفصل الأول منه شاملاً الجرائم التي تؤلف اعتداءً على سلامة شبكات وأنظمة وتقنيات المعلومات وتحديداً حصر المشرع المصري في هذا الفصل جميع الجرائم المعلوماتية أما الفصل الثاني فقد تضمن الجرائم التي تقترف بواسطة أنظمة وتقنيات المعلومات وهي الاحتيال والاعتداء على بطاقات البنوك وأدوات الدفع الالكتروني.

وجاء الفصل الثالث ليعالج انتهاك الحياة الخاصة إلى جانب المحتوى غير المشروع وفي الفصل الرابع جاءت الجرائم المرتكبة من مدير الموقع في حين تضمن الفصل الخامس المسؤولية الجنائية لمقدمي الخدمات.

وبذلك نختم معالجة الحق المحمي في الجرم المعلوماتي وننتقل لمقاربة ذاتية عناصر الجرم المعلوماتي.

المبحث الثاني

ذاتية عناصر الجرم المعلوماتي

سنتناول في هذا المبحث ذاتية عناصر الجرم المعلوماتي في قانون الجرائم المعلوماتية الأوربي في المطلب الأول ثم نتناول ذاتية هذه العناصر في القانون المقارن والقانون السوري في المطلب الثاني.

المطلب الأول:

ذاتية عناصر الجرم المعلوماتي في قانون الجرائم المعلوماتية الأوربي

---

representation as to the state of mind of—
a. the person making the representation, or
b. any other person.
4. A representation may be express or implied.
5. For the purposes of this section, a representation may be regarded as made if it (or anything implying it) is submitted in any form to any system or device designed to receive, convey, or respond to communications (with or without human intervention).

[48]CYBERCRIME LAWS OF THE UNITED STATES Compiled October 2006 by Al Rees, CCIPS

تناولت المادة الثانية من الاتفاقية الأوربية الاختراق تحت عنوان الوصول غير المشروع ويتحقق الوصول بتمكن المخترق من السيطرة على الحاسوب أي الوصول إلى البيانات المخزنة فيه والقدرة على التأثير عليها سوأ أكان الدخول مباشرة أو عن طريق الانترنت أو الشابكة ولا يعد وصولاً مجرد إرسال رسالة الكترونية أو إرسال ملف لكن ما يسمى بالكوكيز أو ملفات تعريف الارتباط يعد تطبيقها دون رضا المالك أو المرخص له وصولاً ،ومن الطبيعي أن الجرم لا يقع من المالك أو من الشخص المرخص له من المالك بالوصول إلى البيانات ومن الثابت أن إرسال البرمجيات الخبيثة من خلال الشابكة إلى المنظومة يؤلف وصولاً إليها بقطع النظر عن تأثير هذه البرمجيات على البيانات.

والسؤال هل مجرد الدخول دون الاطلاع على أي من البيانات ودون فتح أي تطبيق مع إمكانية الفتح من المخترق يؤلف وصولاً وفقاً للمادة الثانية من الاتفاقية ؟ والإجابة نعم فالاتفاقية تناولت الدخول المجرد ولو لم يعقبه أي إطلاع أو حصول على البيانات.

وتركت الاتفاقية الباب مفتوحاً لاشتراط أن تكون المنظومة محمية من خلال مثلاً ما يسمى بالجدران النارية أو برمجيات مكافحة البرمجيات الخبيثة أو كلمات المرور كما سمحت الاتفاقية باشتراط الوصول من خلال حاسوب أي سمحت باستبعاد الوصول المباشر إلى المنظومة من نطاق التجريم.

وتطلبت الاتفاقية العمد وذلك لاستبعاد الخطأ وإن كان الخطأ من الصعب تصوره في إطار الوصول عير المشروع ويتحقق العمد بإرادة الدخول إلى النظام المعلوماتي فليس مطلوباً إرادة الوصول إلى البيانات الموجودة فيه.

والتأثير أو التلاعب أو التدخل بالبيانات تناولته الاتفاقية في المادة الرابعة كجرم مستقل لا كوصف مشدد كما فعل المشرعين السوري والفرنسي وينجم عن الاستقلال أمكانية توافر اجتماع الجرائم المادي بين جريمتي الوصول وفقاً للمادة الثانية وجريمة التدخل وفقاً للمادة الرابعة.

وصور التدخل تتجسد بالإتلاف والمحو والإفساد والتعديل والتدمير ولو حاولنا وضع قاسم مشترك بين هذه الصور وبعبارة أدق ضابط يجمع بينها يمكن أن نجده في استحالة أو صعوبة التعامل بها إما لأنها لم تعد موجودة أو موجودة لكن بشكل مغاير لها.

وبالتأكيد مسح البيانات أو تغييرها من مالكها أومن المرخص له بذلك لا يجعنا أمام جرم التدخل بالبيانات فالبيانات مال والمال لا يتصور الاعتداء عليه من مالكه إلا في إطار ما يسمى بالجرم المستحيل.

والتدخل جرم عمدي يتطلب إرادة الإتلاف أو المحو لدى الجاني أما الإتلاف غير المقصود أو المحو غير المقصود فلا يؤلف جرم تدخل بالبيانات.

والتدخل بالبيانات له صورة العبث بعمل المنظومة من خلال العبث بالبيانات التي تعمل من خلالها بحيث تتوقف عن العمل أو لا تعود تعمل كالسابق وتتطلب بالتالي تدخلاً تقنياً كي تعود إلى سابق عهدها أي كما كانت عليه قبل العبث بالمنظومة ولعل الصورة المثلى للعبث بالبيانات هي تلك البرمجيات التي تدمر نظام التشغيل أو تحد من سرعته على كل حال الاتفاقية تناولت العبث بالمنظومة باعتباره جرماً مستقلاً عن جرم التدخل بالبيانات في المادة الخامسة من منها وجعلت هذه المادة من التدخل بالبيانات أداة العبث بالمنظومة سواء أكان ذلك بالإتلاف أو المحو أو التغيير أو بالإضافة(إرسال بيانات).

والعبث بالمنظومة جرم عمدي وفقاً للاتفاقية يتطلب إرادة إيقاف عمل المنظومة أو الحد من فاعليتها في أداء المهام المطلوبة منها، كما تناولت المادة الثانية اعتراض البيانات أي الحصول عليها أثناء إرسالها من منظومة إلى منظومة أخرى أو أثناء إرسالها داخل المنظومة من المعالج إلى الشاشة أو الطابعة بواسطة الأجهزة التقنية للتنصت وبصورة خاصة أجهزة اعتراض الموجات الكهرومغناطيسية التي تنبعث من المنظومة.

كما يشمل الاعتراض الحصول على البيانات المخزنة في المنظومة من خلال الوصول المباشر إلى المنظومة بما في ذلك الوصول عن طريق الشبكة المحلية أو الوصول غير المباشر عن طريق الشابكة أو الانترنت.

ويجب أن تتوافر لدى المعترض إرادة الحصول على البيانات فهي بذلك جريمة عمدية وينتفي عنصر الجريمة القانوني إذا تم الحصول على البيانات من أجهزة يجيز لها القانون مراقبة البيانات أو إذا تمت المراقبة بقرار من القضاء في إطار جمع الأدلة على الجريمة.

وتحت عنوان سوء استخدام الأدوات تناولت المادة الخامسة من الاتفاقية بالتجريم أدوات الاختراق من حيث الإنتاج أو التوزيع أو الاستعمال أو التداول أو التزويد أو الحيازة سواء أكانت هذه الأدوات برامج أو كلمات مرور.

وهذه الجريمة عمدية أيضاً يجب أن تتجه إرادة المنتج أو الحائز عموماً إلى استعمال أدوات الاختراق في الوصول أو التدخل في البيانات أو النظام أو الاعتراض وتنتفي الجريمة إذا صممت شركة مايكروسوفت مثلاً ،برنامجاً لكسر كلمات المرور بقصد التأكد من قدرة نظام التشغيل ويندوز 12 الجديد على عدم اختراقه.

تتناول المادة السابعة التزوير بنوعيه المادي والمعنوي لوثيقة الكترونية خاصة أو رسمية سواء استعملت كماهي أي كوثيقة الكترونية أو استعملت بعد طباعتها كوثيقة عادية أو رسمية.

وتتناول المادة الثامنة الاحتيال المرتبط بالحاسوب أي التلاعب بقصد التملك لمال الغير في البيانات ذاتها أو في عملية معالجتها أي التلاعب في تطبيق معين كبرنامج وورد أو أكسل أو التلاعب بنظام تشغيل الحاسوب بقصد الحصول على مال الغير.

وعالجت المادة التاسعة حماية الأطفال من الاستغلال الجنسي من خلال تجريم تصويرهم وهم يمارسون الجنس أو محاكاة ذلك أي سواء أكانت الصور واقعية أو مصنعة وذلك بقصد عرض هذه الصور على مواقع الشابكة كما جرمت تلك المادة توفير صور الأطفال الجنسية على مواقع الشابكة فضلاً عن ذلك تناولت المادة أيضاً حيازة تلك الصور الجنسية.

كما حمت الاتفاقية الإنتاج الفكري بكل صوره والعلامات التجارية بمقتضى المادة العاشرة من القرصنة الفكرية الرقمية وبعبارة أدق من الاعتداء عليه بالنشر أو النسخ بواسطة الحاسوب.

وذلك تتمحور ذاتية عناصر الجريمة المعلوماتية في هذه الاتفاقية حول البيانات أو معالجتها من خلال أولاً التأثير عليها وإرادة هذا التأثير أياً كانت صورته إتلافاً أو تدميراً أو محواً أو إفساداً وثانياً الحصول عليها وإرادة هذا التحصيل.

وهذا يسمها كلها بطابع العمد فكلها جرائم عمدية لا مكان بينها للخطأ أياً كان مظهره.

وقد ألحقت هذه الاتفاقية بالجرم المعلوماتي الإعداد له من خلال إنتاج وتوزيع وتزويد أو حيازة تطبيقات وكلمات القرصنة أو الاختراق.

أضافت الاتفاقية تزوير البيانات أو التأثير على البيانات أو معالجتها بقصد التملك لمال الغير ما نفضل أن نسميه التلاعب المعلوماتي.

ولم ينس منظمو الاتفاقية حماية الأطفال من الاستغلال الجنسي وحماية الفكر بمختلف تجسيداته من النشر والنسخ غير المشروع على الشابكة.

وبذلك نكمل مقاربة الاتفاقية الأوربية وننتقل لمعالجة الذاتية في القانون السوري والقانون المقارن.

المطلب الثاني:

ذاتية عناصر الجرم المعلوماتي في القانون المقارن والقانون السوري

جرّم مشرعنا السوري التأثير على البيانات بالحذف أو التعديل باعتباره وصفاً مشدداً لجرم الدخول أو لجرم تجاوز الدخول ،كما جرّم مشرعنا الحصول على البيانات بالنسخ أو الاستخدام أو الإفشاء كوصف مشدد لجرمي الدخول أو تجاوز الدخول.

والواقع أن خطة المشرع السوري في جرم الدخول تلتقي مع خطة المشرعين الفرنسي والمصري لكن ما يميز مشرعنا أنه عدّ التأثير على البيانات أيضاً وصفاً مشدداً لجرم التجاوز خلافاً للمشرع المصري الذي لم يعده وصفاً مشددا[49] بل جرماً مستقلاً باعتبار أن هذا المشرع جرّم التأثير في البيانات بمقتضى المادة 17 من قانون مكافحة جرائم تقنية المعلومات واللافت في هذا السياق أن المشرع الفرنسي كالمشرع المصري جرّم التأثير في البيانات باعتباره جرماً مستقلاً في المادة 323 .3 لكنه لم يجرّم تجاوز الدخول.

أما المشرع الألماني فلم يجرّم الدخول أو تجاوز الدخول بل جرم فقط الحصول على البيانات أو اعتراضها مخالفاً بذلك نظيره الفرنسي الذي لم يجرم اعتراض البيانات أو الحصول عليها.

و لا شك ان تفضيل إحدى العقيدتين أو التقنيتين أي تقنية التوصيف وبالتالي توحيد الجرائم والدمج في جرم واحد أو عقيدة الاستقلال وبالتالي تعدد أو اجتماع الجرائم المادي وهذا التفضيل يعود لفلسفة كل مشرع واعتقد أن التوصيف الذي ينطلق من الحق المعتدى عليه الأهم ويدمج جريمتين بجرم واحد تبعاً للمصلحة الأهم بحيث تصبح أحدهما أداة للأخرى هو منطق قانوني سليم ودقيق في آن معاً.

كما جرمنا مشرعنا السرقة بأدق صورها من خلال تزامن النسخ والحذف (مع التأكيد على أن النسخ لوحدها سرقة لأن من شأنه إنقاص قيمة البيانات باعتباره مالاً أو تبديد قيمتها وإن حافظت على كيانها)أيضاً لا باعتباره جرماً مستقلاً بل وصفاً مشدداً لجرمي الدخول أو تجاوز الدخول.

وقد خص مشرعنا في المادة 18 من القانون(رقم 20 لعام 2202)الحصول على البيانات من خلال الاعتراض باعتباره جرماً مستقلاً دون الاكتراث بما إذا قام المعترض بالنسخ أو الإفشاء أو الاستخدام.

ما يسمى تقنياً بهجوم منع الخدمة جرمه المشرع في المادة الخامسة عشرة من القانون وذلك خلافاً للاتفاقية الأوربية التي عدته صورة من صور التدخل بالنظام[50].

وعلى غرار الاتفاقية جرّم مشرعنا في المادة السادسة عشرة تصميم البرمجيات الخبيثة وترويجها لكن مشرعنا تناول بالتجريم باعتبارها جرائم مستقلة شغل اسم موقع وانتحال الحساب و وإرسال رسائل غير مرغوب بها لكن المشرع الأوربي في الاتفاقية عدها من أفعال التدخل بالبيانات ولم ير فيها جرماً مستقلاً.

وهنا يستوقفنا موقف المشرع الفرنسي الذي لم يجرم التعامل بأدوات القرصنة خلافاً للمشرع الألماني الذي جاء موقفه في المادة 202ج من قانون العقوبات مماثلاً لموقف الاتفاقية الأوربية في المادة السادسة عشرة آنفة الذكر.

ولم يجرم مشرعنا التزوير المعلوماتي باعتباره جرماً مستقلا وإنما عده وصفاً مشدداً لجرمي الدخول أو التجاوز ويتحقق بتعديل البيانات بالحذف أو الإضافة أي تزوير مادي أو اتخذ التعديل صورة التزوير المعنوي وعالج مشرعنا صورة وحيدة لتزوير البيانات وهي تزوير البطاقات الالكترونية في الفقرة ب من المادة 22 من القانون.

ونلاحظ اهتمام المشرعين الألماني والفرنسي بالتزوير المعلوماتي حيث جرمه المشرع الفرنسي في المادة 441-1 من قانون العقوبات كما جرّمه المشرع الألماني في المادتين 269 . 270 وتم إحداثهما بموجب قانون مكافحة الإجرام الاقتصادي الثاني[51]

[49] هذا التجاوز وفقاً للمادة 15 من قانون مكافحة جرائم تقنية المعلومات أما أن يكون من حيث الزمن أو مستوى الدخول.

[50] Adrian HaaseComputerkriminalitätimEuropäischenStrafrecht Mohr SiebeckTübingen2017S. 151

[51] ZweitesGesetzzurBekämpfung der Wirtschaftskriminalitätvom 15.05.1986

PirminSchmidComputerhacken und materiellesStrafrecht- unterbesondererBerücksichtigung von § 202a StGB2001 S.22

لعام 1986 باعتبار أن البيانات المخزنة في الحاسوب تفتقر إلى الإدراك البصري وبالتالي إلى خاصية الثبات المطلوبة في المستند العادي ولم يكن كافياً أن هذه البيانات يمكن مشاهدتها من خلال الحاسوب[52].

والواقع أن المادة 270 من قانون العقوبات الألماني تناولت تزوير معالج البيانات كما لو تم التلاعب بتطبيق معين وبالتالي تزوير المخرجات الناتجة عنه.

وخلافاً للاتفاقية كرر مشرعنا تجريم بعض الجرائم المجرمة أصلاً في قانون العقوبات وقانون المخدرات هي الجرائم الواقعة على الدستور والنيل من هيبة الدولة أو من مكانتها المالية والاتجار بالمخدرات والإساءة للأديان والذم والقدح والتحقير لمجرد ارتكابها من خلال وسائل التقانة.

أما المحتوى الجنسي فقد تناوله مشرعنا في المادة 26 من القانون تحت عنوان جرائم المساس بالحشمة أو الحياء حيث جرّم معالجة الصوت أو الصورة رقمياً لتصبح منافية للحياء كما جرّم التهديد بنشر الصوت أو الصورة المعالجة أو الحقيقية.

وقد أضاف المشرع في القانون الجديد جريمة لم تكن موجودة في القانون السابق هي جريمة إساءة الائتمان المعلوماتي بنموذج قانوني يحافظ على فكرة إساءة الائتمان باعتبارها حلولاً للأمين محل المالك ويضيف إليها فكرة اختلاس المفقودات أي ما جرمه قانون العقوبات كجرم مستقل عن جرم إساءة الائتمان في المادة 659 منه.

فمثلاً الاحتفاظ بملف معلوماتي تم إرساله عن طريق الغلط من مالكه أو بصورة طارئة أو بقوة قاهرة يؤلف جريمة إساءة ائتمان معلوماتي بينما الاحتفاظ بمال دخل تحت سيطرة الجاني غلطاً أو بصورة طارئة أو بقوة قاهرة يؤلف جريمة اختلاس المفقودات وفقاً للمادة 659 من قانون العقوبات.

وإذا كانت الاتفاقية لم تهتم بنشر معلومات شخصية على مواقع الشابكة فقد جرم مشرعنا ذلك بمقتضى المادة 21 من القانون (رقم20 لعام 2202)،كما جرم صورة دقيقة من صور الاعتداء على الخصوصية تتعلق بالصوت أو الصورة بموجب المادة 23 من القانون (رقم20 لعام 2202) حيث جنحت هذه المادة أي عدته جنحة التسجيل للصوت أو الصورة بواسطة وسائل تقنية دون رضا مالك الصوت أو الصورة سواء أكان ذلك من قبل أي شخص أو من مساعدي الضبط العدلي لكنها أجازت التسجيل دون الرضا في حالة واحدة وذلك وفقاً للأصل العام المكرس بقانون الأصول الجزائية أي بقرار من القضاء.

الاحتيال المعلوماتي جرمه المشرع السوري في مادتين الأولى المادة 19 من القانون تحت عنوان الاحتيال المعلوماتي ،والثانية في المادة 22 من القانون تحت عنوان الجرائم المتعلقة بالبطاقة الالكترونية وفي كلا المادتين لم يظهر النموذج القانوني للتلاعب المعلوماتي القائم على التأثير على البيانات أو على معالج البيانات.

فنلاحظ العبارة التي عبر بها عن النشاط الجرمي في الاحتيال المعلوماتي عبارة مرنة وهي عبارة "استخدام وسائل تقانة المعلومات للاستيلاء احتيالاً " في المادة 19 من القانون وعبارة استعمال بطاقة مقلدة أو مزورة أو مزيفة أو مفقودة أو مسروقة أو سلمت له على سبيل الحيازة الناقصة إذا أفضى الاستعمال إلى تحقيق منفعة مادية وذلك في الفقرتين ج . د من المادة 22 من القانون.

والجاني في الحالين يؤثر على البيانات أو على معالج البيانات للحصول على مال الغير وكان الأفضل أن تظهر حقيقة النشاط الجرمي في نص المادة وهي التأثير للحصول على مال الغير خصوصا أن العبارة المستخدمة في المادة 19 من القانون تدل على

[52]Jan Vetter Gesetzeslückenbei der InternetkriminalitätStuttgart 2002 S.47

الاحتيال العادي بواسطة التقانة لا على التلاعب المعلوماتي، فما يميز الاحتيال عن التلاعب المعلوماتي هو محل الجريمة فالمحل في الاحتيال هو الإنسان بينما المحل في التلاعب هو البيانات أو معالج البيانات.

من هذا المنطلق تصبح تسمية التلاعب أدق من تسمية الاحتيال باعتبار أن التلاعب يقع على مادة لا على عقل الإنسان.

كما جرّم المشرع السوري في الفقرة الأولى من المادة 22 من القانون ما بات يعرف بـ "التصيد" وهو الحصول على بيانات بطاقة الكترونية بواسطة وسائل التقانة وهو ما لم تجرمه الاتفاقية باعتباره يؤلف احتيالاً عاديا فالمعتدى عليه هو إنسان تم إيهامه بواسطة وسائل التقانة.

وعلى الرغم من أن المشرعين الفرنسي والمصري جرّما التأثير في البيانات أو في معالج البيانات إلا أنهما لم يجرّما الاحتيال المعلوماتي ويبدو أن المشرع الألماني كان الأقدر على تحديد النموذج القانوني لهذه الجريمة فلو راجعنا خطة المشرع الألماني في المادة 236أ سنجد ما يلي:

خداع الضحية من خلال الحاسوب يؤلف احتيالاً عادياً normaler Betrug لكن نكون أمام جريمتي احتيال عادي وفقاً للمادة 263 واحتيال حاسوبي وفقاً للمادة 263أ إذا تم تسليم المال نتيجة رد فعل الحاسوب المرتبط بالتلاعب ورد فعل الضحية المخدوع.

ونطبق في هذه الحالة الاحتيال العادي لأن الاحتيال الحاسوبي جرم احتياطي Auffangfunktion أو تابع وجد لسد ثغرة قانونية.subsidiarity

Wurde der Vermögensschadenaberdurch die manipulationsbedingteReaktion des Computers und die täuschungsbedingteVerfügung des Menschen gemeinsamherbeigeführt, sind § 263 und § 263 a erfüllt

والواقع هذه فكرة خيالية فالاحتيال العادي يختلف جذرياً عن الاحتيال الحاسوبي وهذا الاختلاف هو الذي دفع المشرع الألماني إلى إيجاد وتقنين الاحتيال الحاسوبي واختلاف النشاط يعني اجتماع مادي للجرائم ولكن هل يمكننا تصور تسليم المال بسبب هذين النشاطين المختلفين؟.

SachlichunterscheidensichBetrug und Computerbetrugnur in einemPunkt: BeimBetrugwirdein Mensch getäuscht, beimComputerbetrugwirdein Computer „getäuscht“ Täuschung“ aufunwahreAngabengegenüber Menschen festgelegtist.

إيهام شخص بمعلومات غير حقيقة لا يتحقق في إطار الكمبيوتر لذلك خداع الكمبيوتر ليس خداعاً وفقاً للمادة 263 لأن الكمبيوتر لا يوهم .

البنية المرئية للاحتيال العادي والاحتيال الحاسوبي واحدة وتم في صياغة المادة 263أ مراعاة عنصر الإيهام والغلط والوصول لملكية الغير.

المصلحة المحمية واحدة المال و لا يمكن إنكار دور المعلومات في الحياة العامة والفردية وضرورة حمايتها من إساءة الاستعمال والتخريب و عدم الثقة بها.

حمايتها للبيانات أي المادة 263أ كمصلحة فوق الفردية لا يغير من شخصيتها أو بنيتها كجريمة أموال. Individualgut أي كجريمة ضد مصلحة فردية.

أيضاً تنتمي هذه الجريمة إلى الاقتصاد وتندرج ضمن قانون العقوبات الاقتصادي وتختص المحاكم الاقتصادية بها ومع ذلك لا يمكن أن نستنتج أن الاقتصاد بات هو المصلحة المحمية.

بنية الاحتيال الحاسوبي تظهر من خلال صور النشاط الجرمي التي تتفرع إلى أربع صور[53]:

[53]Wolfgang MitschStrafrechtBesondererTeil 2 Vermogensdelikte(Randbereich) Teilband 2Springer-Verlag 2001 S.154

1. تصميم خاطئ للبرنامج(معالجة أو طريقة عمله غير صحيحة) التلاعب بالبرنامج هو تلاعب بالبيانات أي التلاعب بالبيانات التي يحتويها إذا كانت بياناته تم التلاعب بها وفقاً لوظيفته فالبرنامج عبارة عن تعليمات عمل للحاسوب والتي يتم تنفيذها من خلال معالجة المدخلات وإنتاج بيانات جديدة أي المخرجات.

البرنامج الصحيح هو البرنامج الذي يعمل ببيانات إدخال صحيحة وبيانات إخراج صحيحة و تتم فيه معالجة البيانات بشكل صحيح.

التلاعب بالبرنامج يعني أن تؤدي معالجة البيانات المدخلة والصحيحة إلى بيانات أو مخرجات غير صحيحة مثلاً إذا تم إدخال 3+3=3

2. البيانات المدخلة غير صحيحة أو ناقصة أو التلاعب بالإدخال في هذه الصورة الثانية للنشاط الجرمي المعالجة صحيحة لكن البيانات المدخلة غير صحيحة أو ناقصة فتؤدي إلى مخرجات غير صحيحة.

3. في هذه الصورة الثالثة للنشاط الجرمي لا يوجد احتيال لأن البيانات صحيحة لكن الجاني لا يملك سلطة استخدامها بالتالي محل الخداع سلطة الجاني باستخدام البيانات. كمن يسرق بطاقة ويستخدمها أو يسحب مبلغ من الصراف من حسابه المكشوف أو يسحب ببطاقة صديقه مبلغ أكبر من المبلغ الذي طلب منه سحبه مثلاً سحب 200 ألف ليرة وهو مفوض بسحب 100 ألف ليرة.

4. التأثير غير المسموح الآخر على سير البيانات: هذه الصورة الرابعة هي صورة احتياطية Auffangtatbestand المراد منها تغطية أي تأثير على البيانات لا يندرج ضمن الصور الثلاثة السابقة وهذا بسبب استخدام المشرع لعبارة "آخر (sonst) Wort ووفقاً للمحكمة الاتحادية الألمانية تتحقق هذه الصورة باللعب الفارغ بآلة النقود الآلية Leerspielen von Geldspielautomaten

والفقه منقسم فبعض الفقه يطبق الصورة الثالثة على هذا الفعل وبعض الفقه يرى عدم تطبيق أية صورة من صور المادة 263أ.ولتوضيح الفكرة نسوق المثال التالي:

(م) مهندس حاسوب وعلى علم ببرنامج تشغيل آلة النقود بالتحديد يعلم في أي مرحلة من مسار اللعبة يجب الضغط على ما يسمى بزر أو مفتاح المخاطرة لكي يحصل على ربح عال.(م) جرب معرفته في آلة نقود عائدة لـ (ص) وحصل على مال منها.

يرفض الفقه تجريمه وفقاً للصورة الثالثة لأن الصورة الثالثة تتطلب إدخال بيانات في معالج البيانات ثم يقوم الحاسوب بمعالجتها وإنتاج مخرجات منها ويؤكد الفقه صحة اتجاه المحكمة العليا في التجريم على أساس الفقرة الرابعة.

والواقع أن التجريم على أساس الصورة الثالثة أدق باعتبار الضغط على زر المخاطرة في المرحلة المحددة أي في الوقت الملائم يؤثر على مسار اللعبة وهو إدخال للبيانات للحاسوب ومن ثم قام الحاسوب بمعالجتها ومكن (م) من الربح ولو لم يضغط أو ضغط شخص آخر لتغير مسار اللعبة وقد يتحقق أو لا يتحقق الربح.

. التأثير على نتائج الحاسوب أو معالج البيانات هذا العنصر هو العنصر التقني أو الحاسوبي المقابل أو الموازي لعنصر الغلط أو الصورة الذهنية Vorstellungsbild في الاحتيال العادي. فالمحتال يؤثر على الصورة الذهنية لدى المخدوع أو الضحية.

وبسبب الخداع حدث الغلط لولا الخداع لانعدمت الصورة الذهنية أو بدت مختلفة ما يعرف قانونياً بالرابطة السببية بين الخداع والغلط. Kausalzusammenhang

بعبارة أدق في الاحتيال العادي يستخدم المحتال العبارات الشفهية أو سلوك معين بينما يستخدم بيانات الكمبيوتر في الاحتيال الحاسوبي ودون هذه البيانات ستبدو المخرجات مختلفة.

Dennis BockStrafrechtBesondererTeil 2VermögensdelikteSpringer-Verlag 2018 S.242

الخسارة المالية هي النتيجة الجرمية كالاحتيال العادي ودون تحقق النتيجة نكون أمام شروع.

والعنصر المعنوي في الاحتيال بنوعيه إرادة التملك المرادفة لإرادة الإثراء Bereicherungsabsicht وبذلك تكتمل مقاربة المشرع الألماني للاحتيال المعلوماتي.

أخيراً بالنسبة للبقاء عمداً في منظومة معلوماتية بعد الدخول إليها عن غير قصد فقد جرمه المشرعان الفرنسي في المادة 323 .1 من قانون العقوبات والمصري في المادة 14 من قانون مكافحة جرائم تقنية المعلومات ولم يجرمه مشرعنا السوري.

وبالنسبة لعنصر الجريمة المعلوماتية المعنوي، القصد هو الصورة الوحيدة للعنصر المعنوي في الجرم المعلوماتي سواء في القانون السوري أو القوانين المقارنة.

النتائج:

بعد هذا التحليل والتأصيل لذاتية الحق المعتدى عليه في الجرم المعلوماتي ولذاتية عناصر هذا الجرم نخلص إلى النتائج التالية:

أولاً: لاحظنا مدى تخبط المشرعين في تحديد صور الجرم المعلوماتي فبعضهم جرّم الدخول إلى منظومة معلوماتية كالمشرع السوري والمصري والفرنسي والانجليزي والأمريكي وبعضهم كالمشرع الألماني لم يجرّم الدخول إلى المنظومة المعلوماتية وإنما جرّم الحصول على البيانات أو اعتراضها.

بعض المشرعين بالغ في التجريم كالمشرع السوري والمشرع المصري فجرّما تجاوز حدود الدخول المشروع أما المشرع الفرنسي والمشرع المصري فقد اهتما بتجريم البقاء في منظومة معلوماتية.

وعلى الرغم من محورية التأثير على البيانات لم يجرمها المشرع السوري إلا كوصف مشدد لجريمة الدخول غير المشروع أو جريمة تجاوز حدود الدخول المشروع.

أيضا لم يجرّم مشرعنا التدخل في منظومة معلوماتية إلا بصورة عابرة وضمن ما يسمى بإعاقة أو منع الوصول للخدمة(المادة 15)،أو من خلال البرمجيات الخبيثة (فقرة ب من المادة 16)،وهو ما اهتم بتجرّيمه صراحةً المشرع الفرنسي والمشرع الألماني والاتفاقية الأوربية كما جرمه المشرع المصري في المادة 17 من قانون مكافحة جرائم تقنية المعلومات بشكل غير مباشر من خلال تجريم تعديل مسار البيانات و البرامج .

أيضاً كرر مشرعتا بعض الجرائم في القانون رقم 20 لعام 2022 لمجرد ارتكابها بواسطة وسائل تقانة المعلومات مع أنها لا تختلف في نموذجها القانوني عن مثيلاتها في قانون العقوبات.

ثانياً: تأصيلياً البيانات أو معالج البيانات مال منقول والاعتداء عليها أو على معالج البيانات هو اعتداء على مال وبالتالي الحق المعتدى عليه هو المال ومحل الاعتداء هو مال أيضاً ،أما الاعتداء على البيانات كأدلة إثبات فلا يوجد أدنى اختلاف بين الوثيقة الورقية والوثيقة الرقمية والتزوير بنوعيه المادي والمعنوي في أي منهما يؤلف اعتداء على الثقة العامة بالمحررات. سواء أكانت ورقية أو رقمية.

ولو أردنا تأصيل الدخول المجرد أي الدخول دون الحصول أو الاطلاع على أية بيانات باعتبار أن الاطلاع حصول على البيانات لوجدنا أنه يؤلف استعمال مال الغير دون حق وما رأى فيه بعض الشرّاح سرقة طاقة أو عمل الحاسوب.

ولتأكيد حقيقة البيانات يمكن إضافة نص إلى قانون العقوبات في الباب الحادي عشر "الأموال" يوضح حقيقة البيانات باعتبارها مال وإضافة نص إلى الباب الخامس "الجرائم المخلة بالثقة العامة" يضع المحررات الرقمية على قدم المساواة مع المحررات الورقية.

ثالثاً: بالنسبة لما يسمى بالاحتيال المعلوماتي لاحظنا دقة صور النشاط الجرمي الأربعة التي صاغها المشرع الألماني في تحديد النموذج القانوني للجريمة وبالنظر إلى أن مشرعنا لم يوضح النشاط الجرمي في الاحتيال المعلوماتي يمكن الاستفادة من النص الألماني في صياغة النص السوري.

رابعاً: إذا كان المشرع الألماني والاتفاقية قد جرّما بدقة متناهية الاحتيال الحاسوبي أو الاحتيال المرتبط بالحاسوب بالمقابل وجدنا عدم تجريمه من جانب المشرعين الفرنسي والمصري لكن المشكلة كانت في توصيفه بالاحتيال فهذا التوصيف ينال من حقيقة الاحتيال القائمة على خلق صورة ذهنية مخالفة للواقع ،صورة محلها العقل الإنساني وهذا لا يمكن تصوره في إطار بيانات الحاسوب ولا حتى في إطار معالج البيانات والواقع أن التوصيف الدقيق كما نراه هو التلاعب المعلوماتي.

خمساً: أبرز الفقه الألماني الذاتية الاقتصادية لبعض الجرائم المعلوماتية سيما وأنها جرمت في سياق قانون حمل اسم مكافحة الإجرام الاقتصادي والواقع لا يمكن إنكار البعد الاقتصادي المتمثل بأثر هذه الجرائم على الأموال وبصورة خاصة أثرها على المؤسسات المالية.

سادساً: العقلية الجرمية التي تقف وراء الجرم المعلوماتي كما حددتها الاتفاقية الأوربية والقوانين المقارنة كانت النية أو الإرادة وهذا يبدو منطقيا فلا إمكانية لتصور الخطأ كصورة للعنصر المعنوي في الجرم المعلوماتي.

المراجع:

د. أشرف توفيق شمس الدين الحماية الجنائية للمستند الالكتروني دراسة مقارنة الطبعة الأولى دار النهضة العربية 2006

د. علي عبد القادر قهوجي الحماية الجنائية للبيانات المعالجة الكترونياً بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنت المنعقد في جامعة الإمارات العربية المتحدة .كلية الشريعة والقانون . مايو 2000 بحوث المؤتمر المجلد الثاني الطبعة الثالثة 2004

- Adrian Haase Computerkriminalitätim EuropäischenStrafrecht MohrSiebeck Tübingen 2017
- Dennis Bock Strafrecht BesondererTeil 2 Vermögensdelikte Springer-Verlag 2018
- Eoghan Casey Digital Evidence and Computer CrimeForensic Science, Computers and the Internet Third Edition
- Georg KüpperStrafrechtBesondererTeillDeliktegegenRechtsgüter der Person und Gemeinschaft Springer-Verlag Berlin Heidelberg 1996
- Jan Vetter Gesetzeslückenbei der Internetkriminalität Stuttgart 2002
- Michael Heghmanns Strafrechtfüralle Semester BesondererTeil Springer-Verlag 2009
- PirminSchmidComputerhacken und materiellesStrafrecht - unterbesondererBerücksichtigung von § 202a StGB 2001
- Wolfgang MitschStrafrechtBesondererTeil 2Vermogensdelikte (Randbereich) Teilband 2 Springer-Verlag 2001
- CONVENTION ON CYBERCRIME Budapest, 23.XI.2001
- Convention on Cybercrime (ETS No. 185) Explanatory Report
- French code penal www.legifrance.gouv.fr
- Strafgesetzbuch www.juris.de