محاضرات في مقياس

الهياكل الإلكترونية

موجهة لطلبة

السنة الأولى ماستر

تخصص: الفلك الفيزيائي

السداسي: الثاني

الموسم الجامعي 2023-2024

الأستاذ: بن احمد محمد

02

مقدمة:

- يشهد العالم اليوم عصرا جديدا يطلق عليه بالعصر المعلوماتي او عصر ثورة المعلومات اولم تعرف البشرية في وقتا ما مثل هذا التدفق الهائل للمعلومة وتزايد سرعتها وعلاقتها بين الناس، فبعد التلغراف والتليفون والراديو والتليفزيون، ثم ظهرت شبكة المعلومات والاتصالات الدولية المتمثلة في شبكة الأنترنت والتي ساهمت بشكل كبير في نقل المعلومات وتبادلها بالصوت والصورة والتي وفرت المال والوقت والجهد، فأصبح في متناول قطاع عريض من الناس التعرف على المعلومات والبيانات بسهولة ويسر

- وأكثر من ذلك فإن هذه الشبكة تسمح للمستخدمين بالتسوق والشراء من خلالها، ولحتى دفع قيمة تلك السلع أو الخدمات.

- كما أدى التقدم التكنولوجي الهائل في مجال تكنولوجيا الإعلام والاتصال وصناعة الحواسيب إلى انتشار هذه التقنية في كافة نواحي الحياة، حتى أصبح لا غنى للإنسان عنها، لكن بالمقابل نتج عن إساءة استخدام هذه التكنولوجيا وهذه التقنية إلى ظهور جرائم مستحدثة وجديدة تختلف في مفهومها وأركانها وطرق ارتكابها عن الجرائم التقليدية المعروفة

- من جانب آخر، خلق هذا النوع الجديد من الجرائم طائفة صعوبات بالغة سواء على مستوى التجريم والعقاب أو على مستوى الإجراءات المتعلقة بالبحث والتحري والتحقيق فيها.

* فالمعلوماتية أصبحت واقعة الجميع ولم تعد ظاهرة محدودة النطاق مقصورة على قطاع تقني محدد، بل ترتب على تزايد عدد المتعاملين بها ومنهم بالطبع رجال القانون ضرورة تدخل القانون، وهذا الأخير له دوره في الاهتمام بهذه الظاهرة المستحدثة والتفاعل معها، فالعلاقة تبدو وثيقة بين المعلوماتية والقانون.

* وتعتبر الجريمة المرتكبة عبر الانترنت تأخر الأنظمة السابقة التي خلفتها التقنية العالية للمعلوماتية، حيث أخذت هذه الأخيرة حيزا كبيرا من الدراسات من أجل تحديد مفهومها مما أنجر عنه وضع عدة مصطلحات للدلالة عليها من بينها (جرائم الحاسوب - جرائم التقنية العالية - جرائم المعلوماتية - جرائم الغش المعلوماتي - وصولا الى جرائم الانترنت ... وغيرها).

* ولذلك ارتأينا أن نقسم هذه الدراسة في الإجرام المعلوماتي (الالكتروني) إلى دراسة ماهية هذا النوع من الجريمة، ثم نتطرق الى الجوانب الموضوعية وما جاء به المشرع الجزائري في مجال النصوص القانونية المتعلقة بمكافحتها.

- القسم الأول : ماهية الجريمة الإلكترونية (المعلوماتية)

تمهيد :

- لا يمكن للمشرع في سياسته الجنائية أن يضع الأحكام الموضوعية المتعلقة بالتجريم والعقاب بخصوص أي جريمة مالم يدرسها دراسة معمقة من مختلف جوانبها وهذا قصد تحديد مفهومها وبيان أركانها وأساليب إرتكابها.

- وقصد الإلمام بماهية الجريمة المعلوماتية سنتطرق إلى الحديث عن :

أولا : ظاهرة المعلوماتية في مجال الجريمة.

ثانيا : مفهوم الجريمة المعلوماتية.

أولاً: خلفية المعلوماتية في مجال الجريمة:

- تتعلق الجريمة المعلوماتية أساساً بالمعلومات، ولذلك كان من المهم وضع نطاق محدد حول ماهية المعلومة التي تتعلق أساساً بالجريمة المعلوماتية، وهل لهذه الأخيرة طبيعة خاصة تميزها عن غيرها؟
وبمعنى آخر ما هو الوضع القانوني لهذه المعلومات؟
ثم هل لهذه المعلومات قيمة في ذاتها بحيث يمكن اعتبارها محلاً للاعتداء عليها أم لا؟

---

(1) مفهوم المعلومات وتقنية المعلومات:

أنّ توجد علاقة بين الحاسب الآلي وارتكاب الجرائم الحديثة هو نتيجة طبيعية للتطور التكنولوجي، وإذا كانت الجريمة المعلوماتية تتعلق أساساً بالمعلومات وهي وقيمة، وعليه فهذا الأساس سوى نتناول هنا مفهوم كل من (المعلومات) ثم (تقنية المعلومات). X

أ) - تعريف المعلومات:

- المعلومات كلمة شائعة منذ خمسينات القرن التاسع عشر، وتم استعمالها في مجالات مختلفة، مما جعل لها في الاستعمال الدارج مفاهيم عديدة ومتنوعة.

- وهي من حيث اللغة فإنها مشتقة من كلمة (علم) وذلك لأنها هي المعرفة التي يمكن اكتسابها ونقلها

05

* ومن الوجهة الإصطلاحية ثمة تعريفات كثيرة وعديدة للمعلومات وضعها باحثون من تخصصات وثقافات مختلفة.
ولعل أكثر التعريفات التي قيلت في المعلومات نجد:

- "اتها: مجموعة من المعطيات والبيانات المعالجة آليا والتي تم تخزينها وفق نظم تكنولوجية من أجل الحفاظ عليها والرجوع إليها وقت الحاجة، وهذه المعطيات والبيانات يمكن أن تكون لها علاقة بأشخاص أو أموال، كما يمكن أن تكون لها علاقة بأمور أمنية أو سياسية أو اقتصادية أو تجارية ... »

- كما يمكن أن يفهم من مصطلح المعلومة مفهوما ضيقا كما هو الحال في مجال التكنولوجيا، فإن لها مفاهيم عديدة كالرسالة والإشارة والأخبار والوثائق والصور والأرقام والعلامات وغيرها... والتي تصلح أن تكون محلها محلا للتبادل أو للإتصال أو للمعالجة الآلية.

- وإن العلاقة بين المعلومة (l'information) والمعلوماتية (l'informatique) فهذه الأخيرة هي المعالجة الآلية للمعلومة أي تجميع ومعالجة المعلومة تكنولوجيا ثم تخزينها أو استرجاعها وإرسالها مرة أخرى.

- وعموما فإن المعلوماتية هي التعامل الفوري والسريع مع المعلومة.

* وعليه تعتبر المعلومة من أهم العناصر التي تقوم عليها الأجرام الإلكترونية، زيادة إلى العناصر والأركان المعروفة لقيام الأجرام عموما، لذا وجب علينا في هذا المقام أن نتطرق إلى أهم الشروط الواجب توافرها في المعلومة من أجل وضع إطار قانوني لحمايتها

* ولعل من بين أهم هذه الشروط نجد ما يلي :

1- أن يتوافر في المعلومة التحديد والابتكار :

- فالمعلومة التي تفتقر إلى صفة التحديد (precise) لا يمكن حمايتها بالمعنى الدقيق، لذا يجب أن تكون المعلومة محددة، أي ضرورة حصرها في نطاق معين.

- كما يجب أن تكون المعلومة مبتكرة، أي أنها تحمل صفة الإبتكار (Originale) مما يعطيها نوع من الخصوصية بحيث أن لا تكون عامة ومتاحة للجميع وهذا ما يجعل المعلومة تتسم بالأصالة ولم تكن موجودة من قبل لأن المعلومة المتاحة يمكن الوصول إليها من قبل أي شخص.

2- أن يتوافر في المعلومة السرية والاستئثار :

- فهنا يجب أن تكون المعلومة محاطة بجدار من السرية أي ضرورة الاحتفاظ بهذه المعلومة في نطاق محدد من الأشخاص، مما يجعل منها معلومة غير مفصح عنها، وبالتالي فإن المعلومات التي لا تتصف بالسرية هي معلومات عامة ومتاحة بين الناس، إذن فإن صفة السرية

لازمة للمعلومة حتى يمكن حمايتها.

- أما الإستئثار بالمعلومة قد يرجع إلى سلطة شخص ما على المعلومة في التصرف فيها (كالأموال) أو تكتسب المعلومة هذه الصفة الأخيرة إما بإرادة الشخص أو بحسب طبيعتها أو بإجتماع الأمرين معا ومثاله الرقم السري للبطاقة الإئتمانية.

3- القيمة القانونية للمعلومة:

وهذه القيمة القانونية قد تختلف من معلومة إلى أخرى بحيث هناك قيم قانونية مختلفة بحسب نوع كل معلومة مثلا (قيمة تجارية، قيمة فكرية، قيمة مالية ... إلخ)

4- الحماية الجنائية المقررة للمعلومة:

في هذه الحالة عندما تتوافر كافة الشروط السابقة مجتمعة فإنه يتعين أن ترصد حماية جنائية للمعلومات، وهي إتخاذ كافة الإجراءات الكفيلة بالمحافظة على هذه المعلومات ومنع كل أنواع الإعتداء والتعرض لها تحت طائلة الجزاء الجنائي.

- وهذا ما إتجهت له المشرع الجزائري بموجب قانون العقوبات والذي سوف نفصله في حينه.

ب) تعريف تقنية المعلومات :

- يمكن القول هنا أن المعلوماتية أو تقنية المعلومات هي علم التفاعل الآلي على الأخص بواسطة الآلات أو توماتيكية مع المعلومات باعتبارها دعامة للمعارف الإنسانية وأساس للإتصالات في ميادين عديدة.
- كما يعرى البعض هذه التقنية بأنها ذلك التزاوج والإلتحام بين تكنولوجيا الحواسيب بمختلف أنواعها مع الاتصالات الحديثة، والاستعمال المتزايد للإليكترونيات في العماليات الصناعية والتجارية والخدمات.
- ولذلك يرى البعض أن المعلوماتية يحكمها قانون يسمى بقانون المعلومات (قانون تقنية المعلومات) وهو مجموعة من القواعد و الأحكام الموجودة في شتى فروع القانون الأخرى والتي يمكن تطبيقها على المسألة المعلوماتية بحسب نوع المشكلة المثارة التي قد تخضع لأحكام قانونية متعددة.
- وعي إينا أن المعلوماتية يقصد بها مجموع النظم والشبكات ووسائل المعلومات والحواسب والبرمجيات والإنترنت ومختلف الأنشطة المتعلقة بها.

09

② الجريمة المعلوماتية والمجرم المعلوماتي :

- تحتل المعلومات مكانة متميزة في العصر الحالي، فأصبحت محورا لأي دراسة تتعلق بالمعلوماتية وهذا بوصفها علم معالجة المعلومات وكذا باعتبارها وسيلة ناقلة للمعارف الإنسانية.
- وقد أدى الإستخدام المتزايد للأنظمة المعلوماتية إلى ظهور فوائد عديدة وعظيمة في مجال التقدم التكنولوجي فأصبحت المعلومات قيمة إقتصادية وسلعة تباع وتشترى. كما نتج عن هذا الإستخدام للمتزايد الكثير من المخاطر منها على سبيل المثال السرقة والإحتيال والتجسس واتلاف المعلومات والبرامج وغيرها من الجرائم المعلوماتية الأخرى التي لا حصر لها في الوقت الراهن.
- ولذلك فإن الجرائم المعلوماتية هي الثمرة الخبيثة الناتجة عن التقدم السريع في تكنولوجيا المعلومات بمختلف المجالات العلمية الذي يتميز به عصرنا الحالي.
- وبهذا نرى أنه لابد من تحديد مفهوم للجريمة المعلوماتية وكذا مفهوم للمجرم المعلوماتي وهذا على النحو التالي :

2) مفهوم الجريمة المعلوماتية (الإلكترونية):

- لقد دخل في قاموس الجرائم نوعاً جديداً يطلق عليه معظم الدول (بالجريمة المعلوماتية) أو (الجريمة الإلكترونية) أي تلك الأعمال والأفعال التي تتم عن طريق استخدام الحواسيب والإنترنت، وهي من أخطر التحديات التي تواجه التعاملات الإليكترونية اليوم.
- ومما لا شك فيه أن هذا النوع من الجرائم إزداد بقوة خلال السنوات القليلة الماضية ونجح المجرمون في إبتكار العديد من الوسائل للقيام بعملياتهم الإحتيالية بدقة فائقة.
- وعليه سوف نتطرق الى تعريف هذه الجريمة وتبيان أهم خصائصها التي تتميز بها.

1- تعريف الجريمة المعلوماتية:

- نظراً للطبيعة الخاصة للجرائم الإلكترونية، إختلف الفقه الحديث في وضع تعريف جامع ومانع لها.
- لذا سوف نركز على بعض التعاريف التي تناولها الفقه والتي من أهمها نجد:

* إن الجريمة المعلوماتية أو الإلكترونية هي كل نشاط غير مشروع موجه للمساس بالمعلومات المخزنة داخل الحاسوب

- وعرفتا أيضاً بأنها: « جرائم ضد المال مرتبط باستخدام المعالجة الآلية للمعلوماتية ».
- وقيل عنها: « كل فعل إجرامي متعمد أياً كانت صلته بالمعلوماتية ينشأ عنه خسارة تلحق بالمجني عليه وكسب يحققه الجاني ».
- وعرفتا أنها: « الجرائم التي تلعب فيها البيانات والبرامج المعلوماتية دوراً رئيسياً ».
- كما قيل عنها: « كل أشكال السلوك غير المشروع أو الضار بالمجتمع الذي يرتكب باستخدام الحاسوب ».
- أو أنها: « كل سلوك ينطوي على استخدام الأجهزة التقنية الحديثة أو أحد ملحقاتها أو برامجها في ارتكاب أغراض غير مشروعة ».
- ويمكن في الأخير أن نتبنى التعريف الذي أقره المؤتمر العاشر للأمم المتحدة لمنع الجريمة حول جرائم الحاسوب وشبكة الإنترنت والذي عقد بفيينا في 2000/04/17 إذ عرف الجريمة المعلوماتية بأنها: « جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية وتشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية ».

* ومن خلال هذه التعاريف وغيرها من التعريفات التي قيلت في الجريمة المعلوماتية نستنتج الحقيقة التالية: من الصعوبة بمكان وضع تعريف لهذه الظاهرة الإجرامية وذلك لخشية حصرها في مجال ضيق في ظل التطور الحاصل في العالم

8- خصائص الجريمة المعلوماتية:

- تتميز هذه النوعية من الجرائم بجملة سمات تتصف بها عن غيرها من الجرائم التقليدية الأخرى.
وهذا بسبب إرتباط هذه الجريمة بجهاز الحاسوب وشبكة الإنترنت، وهذا ما أضفى عليها مجموعة من الخصائص يمكن إجمالها في الآتي:

* أنها جريمة عابرة للحدود الوطنية:

- وهذا لأن المجتمع المعلوماتي أو كما يعرف بمجتمع الإنترنت (العالم الافتراضي) لا يعترف بالحدود الجغرافية، وذلك بالنظر إلى عالمية الشبكة العنكبوتية، فهو مجتمع منفتح عبر شبكات تخترق الزمان والمكان، دون أن تخضع للمراسة، وهذا ما يؤدي بنا إلى نتيجة مفادها أن الجاني قد يتواجد في دول مختلفة قد تفصل بالجريمة المعلوماتية الواحدة وفي آن واحد. إذ غالبا ما يكون الجاني في بلد والمجني عليه في بلد آخر، بعد أن سهلت الإنترنت الأمر التنقل والاتصال عبر فضاءاتها الواسع.

- وهذه الطبيعة التي تتميز بها هذه الجريمة في كونها عابرة للحدود الدولية ولا تعترف بها ولا بتراعيها، خلقت العديد من المشاكل حول تحديد الدولة صاحبة الاختصاص القضائي بهذه الجريمة، وكذلك حول تحديد القانون الواجب التطبيق وغير ذلك من النقاط التي تثيرها الجرائم المنظمة والعابرة للحدود بشكل عام.

* أنها صعبت الإكتشاف:

- تتميز أيضا الجريمة المعلوماتية بصعوبة إكتشافها وعادة ما يكون إكتشافها بمحض الصدفة فقط.
وهذا إذا ما قورنت بما يتم إكتشافه من الجرائم التقليدية، ويمكن رد الأسباب التي تقف وراء الصعوبة في إكتشاف الجرائم المعلوماتية مثل:

- هو عدم ترك هذا النوع من الإجرام لأي أثر خارجي بحيث يستطيع الجاني تدمير أدلة الإدانة في أقل من ثانية واحدة، مما يخلق صعوبات بالغة لسلطات البحث والتحري والتحقيق في ملاحقة الجاني وحتى عدم إفلاته من العقاب.

- كما يقف وراء الصعوبة في إكتشاف الجرائم المعلوماتية من خلال الدور السلبي الذي يلعبه المجني عليه، حيث أن أغلب الضحايا من هذه الجريمة يمتنعون عن التبليغ عنها وهذا أيضا راجع إلى سببين أولهما صعوبة تحديد هوية المجرم الإلكتروني الذي بدوره يستطيع التخفي عن طريق القدرة والمعرفة والخبرة بمجال الحاسب الآلي والإنترنت.

- والسبب الثاني له علاقة باعتبارات شخصية ومالية أو حتى متعلقة بسمعة المجني عليه كالشركات وغيرها،

* أنها جريمة يصعب إثباتها بسهولة:

- حتى ولو تم إكتشاف أو الإبلاغ عن الجريمة المعلوماتية فإنه يصعب أحياناً إثباتها بسهولة وهذا نظراً للطابع الخاص الذي تتميز به هذه الجريمة.

فإن إثباتها يحيط به كثير من الصعوبات التي تواجه سلطة الاستدلال أو التحقيق الجنائي في إستخلاص الدليل الجنائي.

- ويعود ذلك لعدة أسباب أهمها:

* الجرائم المعلوماتية لا تترك أثراً خارجياً، فلا عنف فيها ولا سفك دماء، ولا أثار لإقتحام لسرقة الأموال منها وإنما هي أرقام وبيانات تتغير أو تمحى من السجلات المخزنة في الذاكرة وليس لها أي أثر خارجي مرئي.

* الجرائم المعلوماتية هي جرائم فنية تتطلب تخصصاً معيناً في مجال الحاسوب الآلي، فهي تتم في بيئة غير تقليدية، حيث تقع خارج إطار الواقع المادي الملموس، أي أن مسرح الجريمة المعلوماتية هو الحاسوب والإنترنت، مما يجعل الأمور تزداد تعقيداً لدى سلطات الأمن وأجهزة التحقيق والملاحقة، وبالتالي فإن أمر طمس الدليل الإلكتروني أو محوه كلياً من قبل الفاعل أمراً في غاية السهولة.

* الجرائم المعلوماتية يصعب إثباتها من طرق الجهات المختصة وهذا بسبب نقص الخبرة الفنية والتقنية لدى رجال الشرطة والقضاء، لذلك تسعى الدولة جاهدة في تدريب وتأهيل الجهات المختصة في مجال المعلوماتية.

ب) مفهوم المجرم المعلوماتي ؟

- يُشك أن الشخص الذي يرتكب الفعل غير المشروع ويعتدي فيه على حق من حقوق الغير بالمعنى الواسع يعد في نظر القانون مجرماً ويتعرض للعقاب.

- ولذا كنا في مجال الإجرام المعلوماتي، فإنه يجب علينا أن ننظر إلى المجرم المعلوماتي من عدة زوايا، والتي من بينها الظروف التي دفعته لإرتكاب جريمته وأسبابها والنظر أيضاً إلى صفاته.

(1) تعريف المجرم المعلوماتي ؟

- هو ذلك الشخص الذي يجمع بين إحتراف الحاسب الآلي ومعرفته بالإنترنت، إذ يتمتع بقدرة فائقة وعالية من الذكاء والدراية الواسعة بالتخصصات المتعلقة بالأنظمة المعلوماتية في المجال التقني والإلكتروني.

- لذا يقال عادة "أن الإجرام المعلوماتي هو (إجرام الأذكياء) وهذا مقارنة بالإجرام التقليدي الذي عادة ما يلجأ فيه المجرم إلى إستخدام القوة البدنية والعنف.

- ولكن هذا لا يمنع من أن يوجد مجرم معلوماتي بمعرفة الصدفة دون أن تكون له دراية واسعة بمجال المعلوماتية.

② صفات المجرم المعلوماتي :

- رغم الصعوبات التي قد تظهر عند تحديد سمات معينة للمجرم المعلوماتي بسبب تعدد أجرائم الإلكترونية وتنوعها، فإنه يمكن القول أن المجرم المعلوماتي يتميز بعدة سمات أهمها :

* المجرم المعلوماتي هو انسان إجتماعي بطبعه :

- فالمجرم المعلوماتي يعيش في بيئته الإجتماعية كإنسان بصورة عادية، بل ويحظى بثقة كبيرة في مجال عمله، فهو لا يضع نفسه في حالة عداء مع المجتمع، وشعوره أنه محل ثقة يزيد في دافع الإجرام لديه، كما قد يكون منعزلا لا يميل إلى مخالطة الناس، كما قد يكون من سوابق المجرمين أي معتود الإجرام.

* المجرم المعلوماتي يتمتع بالمهارة والإحتراف والذكاء :

- في غالب الأحيان يكون المجرم المعلوماتي شخص من اقوابغ أي انه انسان ذكي ومحترف ويتمتع بمهارات عالية في مجال الإلكترونيات، فهو يتمتع بمعلومة وخبرة لا يستهان به في تقنيات الحاسوب والإنترنت بل والأكثر من ذلك أن بعضهم من يكون هذه الصناعة هم المتخصصين في مجال المعالجة الآلية للمعلومات،

③- أسباب ودوافع إرتكاب الإجرام المعلوماتي:

من أهم أسباب انتشار الإجرام المعلوماتي نجد مايلي:

* الإنبهار بالتقنية المعلوماتية والرغبة في الاكتشاف والتعلم:

- كشفت معظم الدراسات الاجتماعية أن ظهور هذا النوع من الاجرام قد يكون بدافع الفضول وحب الاكتشاف والمعرفة أو مجرد الهواية واللهو في بداية الأمر وذلك شبيهة الإنبهار بالثورة المعلوماتية وتكنولوجيا المواسيبا، ولذلك فإن هؤلاء ليسوا على جانب كبير من الخطورة الإجرامية، وإنما هم غالبا ما يفضلون تحقيق انتصارات تقنية ودون أن يتوافر لديهم نوايا سيئة.

* الرغبة في الربح المالي والثراء السريع:

- قد تدفع الحاجة البعض الى تحقيق ثراء سريع أي الربح وتحقيق الكسب المالي غير المشروع في زمن قياسي، وهذا عن طريق الإعتداء على معلومات معينة ذات أهمية ولذلك يعد هذا السبب من أكثر الأسباب التي تدفع الى انتشار الإجرام المعلوماتي.

* المؤثرات الشخصية والرغبة في الإنتقام :

- يتأثر الإنسان في بعض الأحيان ببعض المؤثرات الخارجية التي تحيط به، ونتيجة لوجوده داخل البيئة الإلكترونية وعالم الإنترنت تتوافر هذه المؤثرات فإن الأمر سوى يؤول في النهاية إلى إرتكابه جريمة معلوماتية، ولعل من أهم هذه المؤثرات نجد على سبيل المثال الحقد والإنتقام والكراهية سواء ضد شخص معين أو مؤسسة أو حتى نظام بأكمله. فالحقد والكراهية يولدان الإبتزاز المالي فيلجأون إلى أفعال غير مشروعة ضد الأنظمة المعلوماتية.

- أما عامل الإنتقام وذلك عندما يتم فصل عامل من كان له دراية بالمعلوماتية، فإن ذلك قد يهيئ له المناخ لإرتكاب جريمة كأن يدمر البرامج المعلوماتية بالفيروسات والتي ينشأ عنها أضرار جسيمة.

7

القسم الثاني : موقف قانون العقوبات الجزائري من الجريمة المعلوماتية

- يعتبر قانون العقوبات الجزائري من القوانين العربية السباقة الى هذا الموضوع، حيث بادر المشرع الجزائري الى تعديل قانون العقوبات بمقتضى القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 وهذا بإدراج القسم السابع مكرر من المادة 394 مكرر الى 394 مكرر 7 وهذا تحت عنوان « المساس بأنظمة المعالجة الآلية للمعطيات » وذلك رغبة منه الى مواكبة العصرنة والسير قدماً نحو تطوير منظومته التشريعية، حتى يضع سياجاً لحماية خصوصية الأفراد والمجتمع من الاستخدام السيئ للوسائل التكنولوجية الحديثة سواء عن طريق الكمبيوتر أو الهاتف النقال وما يرتبط بها من تقنيات وشبكات، ومن ثم نص على مجموعة من الجرائم، وأوجب لها عقوبات قاسية للحد من إقترافها.

- إلا أنه وقبل الحديث عن هذه الجرائم، لابد من التعرض الى مفهوم نظام المعالجة الآلية للبيانات، ثم نتطرق الى جرائمه وفق ما جاء به قانون العقوبات.

أولا: مفهوم نظام المعالجة الآلية للمعطيات:

- يعتبر نظام المعالجة الآلية للمعطيات (البيانات) ذلك الشرط الأولي والأساسي للبحث في توافر أو عدم توافر أي جريمة من الجرائم الإلكترونية، فإذا تخلف هذا الشرط لا يكون هناك مجال للبحث في مدى توافر أركان أي جريمة من الجرائم الماسة بنظام المعالجة الآلية للمعطيات، إذ أن هذا الشرط يعتبر عنصر لازم لكل منها.
- ولذلك يكون من اللازم تحديد وتعريف هذا الشرط ثم الحديث عن مدى خضوعه للحماية الجنائية.

(1) تعريف نظام المعالجة الآلية للمعطيات:

- إن نظام المعالجة الآلية للمعطيات تعبير فني يصعب على الباحث في مجال القانون إدراك حقيقته وفحواه بسهولة فضلا عن كونه مفهوم متطور يخضع للتطورات السريعة في مجال صناعة تكنولوجيات الإعلام والاتصال. ومع ذلك سوف نذكر هنا أهم التعاريف التي تناولت هذا النظام ومنها:

* أنه : « كل مركب يتكون من وحدة أو مجموعة وحدات معالجة، والتي تتكون كل منها من الذاكرة والبرامج والمعطيات وأجهزة الإدخال والإخراج وأجهزة الربط، والتي تحقق بنية واحدة وهي معالجة البيانات والمعطيات، على أن يكون هذا النظام والمركب لنظام الحماية الفنية ».

* كما عرفه بتعريف آخر وهو أنه : « أي جهاز أو مجموعة من الأجهزة المترابطة أو ذات الصلة يقوم واحد منها أو أكثر بالمعالجة الآلية للمعطيات تنفيذا لبرنامج معين ».

~~[redacted]~~

* وتجدر الإشارة هنا إلى أن المشرع الجزائري هو تناوله للجرائم الإلكترونية سواء في قانون العقوبات أو القوانين المكملة له، استخدم مصطلحين مختلفين في هذا المجال هما مصطلح (نظام المعالجة الآلية للمعطيات) وكذا مصطلح (منظومة معلوماتية) وكلاهما واحد. حيث عرفه بموجب المادة (2) من القانون رقم 09-04 المؤرخ في 05/08/2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، (المنظومة المعلوماتية) على أنها

- « نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين »

- وانطلاقا من هذه التعاريف السابقة نجد أنها قد ركزت في مفهوم هذا النظام على ثلاثة عناصر أساسية وهي :

* العنصر الأول : يتمثل في مجموعة مكونات هذا النظام أو المركب، أي المكونات المادية والمعنوية (وحدات المعالجة ووحدات التخزين أو وحدات الإدخال والإخراج ... وغيرها)

* العنصر الثاني : وهو وجود شبكة من الاتصالات بين هذه الوحدات المادية والمعنوية ويعني ذلك ارتباطها فيما بينها لتشكل نظاما معلوماتيا واحدا، أو مرتبطة بمجموعة من النظم الأخرى والمتصلة فيما بينها بواسطة أجهزة الربط المختلفة سواء عن قرب أو عن بعد والتي تهدف في الأخير إلى تحقيق عمل معين.

* العنصر الثالث : وهو ضرورة وجود نظام حماية فنية أو ما يطلق عليه (بنظام الأمان)، ويعني ذلك ضرورة خضوع هذا النظام (المركب) للحماية الفنية حتى يمكن أن يتمتع بالحماية القانونية الجنائية وذلك باستعمال أسلوب التشفير (الكود) مثلا.

② أهمية إخضاع نظام المعالجة الآلية للمعطيات للحماية الفنية :

- تنقسم الأنظمة المعلوماتية إلى أنظمة مفتوحة للجمهور وأنظمة أخرى قاصرة على أصحاب الحق فيها دون أن يكون للأول حماية فنية لها، بينما الثانية تتمتع بنظام أمان وحماية فنية، وذلك بغرض توفير الأدوات والوسائل والأساليب اللازمة لحماية المعلومات التي تحتويها من المخاطر التي تهددها الداخلية منها أو الخارجية.

- حيث يقصد بمصالح الحماية الفنية للنظام المعلوماتي ذلك الإجراء الوقائي الذي يتخذه صاحب النظام أو صانع البرنامج أثناء وضعه له، وهذا الأخير من الإعدادات التي قد تعيق عليه (كالأرقام السرية) أو (كلمات المرور) و (الكود) و (الشفرات) ... إلخ.

* وعليه يطرح السؤال وهو :

ما مدى خضوع نظام المعالجة الآلية للمعطيات للحماية الفنية ؟ وهل الحماية الجنائية مقصورة على نظام دون الآخر ؟

* وللإجابة على هذا التساؤل برز اتجاهان متعارضان حول مسألة إضفاء الحماية الفنية على النظام المعلوماتي من عدمها.

* الإتجاه المؤيد للحماية الفنية :

- يرى أصحاب هذا الإتجاه أن من الطبيعي حماية النظام المعلوماتي بحسب أن من يقوم بمعالجة معلوماته وتخزينها واستغلالها وجب عليه وضع الوسائل الفنية اللازمة للحماية من كل أنواع الإعتداء و الغش المعلوماتي

- لذا يذهب الرأي الغالب [redacted] مؤيدي هذا الإتجاه إلى ضرورة وجود نظام أمني ، وأن القانون الجنائي لا يحمي إلا الأشخاص الذين لديهم حرص على أموالهم ، ذلك أن القانون يجرم الإعتداء على نظم الأمن المتضمنة في النظام المعلوماتي ، ويستند أنصار هذا الإتجاه لعدة حجج منها ، أن الإعتداء على النظام الأمني شرط مفترض لقيام الجريمة المعلوماتية ، وأن العدالة تقتضي عدم العقاب على فعل يمكن إعتداء على حق لم يتحوط له صاحبه ، فضلاً عن أن التسليم بتجريم محل الأفعال التي تمس بالنظم المحمية وغير المحمية يعني توسع في مجال التجريم ، فمثلاً كل دخول غير مشروع إلى صفحة الكترونية أو موقع ما جريمة ، وذلك أمر غير منطقي .

* الإتجاه المعارض للحماية الفنية :

- لا يشترط أصحاب الإتجاه المعارض وجود نظام الحماية الفنية، وهذا بسبب أن المشرع لم ينص على هذا، وأنه لا يجوز أن تقتصر الحماية الجنائية على الأنظمة المحمية فقط، وإنما يجب أن تمتد لتغطي كل أنظمة المعالجة الآلية للمعطيات المحمية منها والغير المحمية، كون هذا الشرط يؤدي مباشرة إلى الحد من الحماية الجنائية للنظم غير المشمولة بتجهيزات أمنية داخل النظام، وأن الأمر مقصور فقط على النظم المحمية.

- وزاد أنصار هذا الإتجاه إلى القول بأن نظام الأمن المعلوماتي لا يكون له سوى دور واحد فقط وهو إثبات سوء نية من قام بإنتهاك النظام الأمني والدخول إليه بطريقة غير مشروعة، بحيث يدخل ذلك في عداد إثبات القصد الجنائي من عدمه.

* موقف المشرع الجزائري من نظام الحماية الفنية:

- بالنسبة للمشرع الجزائري، نلاحظ من جهة أنه استعمل مصطلح (منظومة) بدلا من مصطلح (نظام) في التعريفات السابقة، وقد أصاب في ذلك بسبب تعدد أنواع الأنظمة المعلوماتية، وهذا لا ينحصر فقط في نظام الحاسوب، بل يتعداه إلى كل نظام أو جهاز يقوم بالمعالجة الآلية للمعطيات ومنها شبكة الأنترنت والبريد الإلكتروني والبطاقات الإلكترونية ...

- وبالتالي ترك المشرع الجزائري الباب مفتوحا في حماية الجنائية للمنظومات المعلوماتية المشمولة بنظام الحماية الفنية المحمية.

* ومن جهة أخرى لم يشترط المشرع لقيام الجريمة المعلوماتية خضوع النظام المعلوماتي للحماية الفنية وبالتالي أخذ بالاتجاه الرافض والمعارض لإضفاء الحماية الفنية على النظام المعلوماتي، حيث يهدي المشرع من وراء ذلك إلى إضفاء الحماية الجنائية على كافة أنظمة المعالجة الآلية للمعطيات بغض النظر عن تمتعها بالحماية الفنية أم لا.

* نضيف إلى ذلك أن النصوص المتعلقة بجرائم الاعتداء على النظام المعلوماتي صدرت دون أن تتضمن شرط الحماية الفنية، لأنه من المبادئ المستقرة في القانون الجنائي أنه لا يجوز تقييد النص المطلق أو تخصيص النص العام.

القسم الثاني: جور الاعتداء على الأنظمة المعالجة آليا للمعطيات:

- يتخذ الاعتداء على النظام المعلوماتي أكثر من شكل ولعل أهمها نجد:

أولا: جريمة الدخول أو البقاء غير المصرح بهما:

- تعد أنشطة الدخول غير المشروع لأنظمة المعالجة الآلية للمعطيات من أكثر الجرائم شيوعا وهو ما نص عليه المشرع الجزائري من خلال نص المادة 394 مكرر من قانون العقوبات بقوله: «... يعاقب بالحبس من ثلاثة (3) أشهر إلى سنة (1) وغرامة من 50,000 دج إلى 200,000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك. تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة. وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة (6) أشهر إلى سنتين (2) والغرامة من 50,000 دج إلى 300,000 دج ».

* من خلال قراءتنا لنص هذه المادة نلاحظ أن المشرع يجرم الدخول وكذلك البقاء في النظام المعلوماتي ومما يتحينا الوقوف عنده هنا هو أن المشرع فرق بين فعل الدخول غير المشروع وبين البقاء دون وجه قانوني.

* ويمكننا إيجاز ذلك إلى سبب بسيط يبرر هذه التفرقة وهو أنه وإن كان الدخول عن طريق الخطأ يستغني عنه الجرم فإن البقاء عن قصد يشكل جرماً قائماً بذاته تم عن إرادة الجاني في إلحاق ضرر بالغير.

(1) الركن المادي للجريمة:

- تتحقق هذه الجريمة بقيام ركنها المادي، فمن خلال إلمامة استقراءنا لنص المادة 394 مكرر 1 ق ع الذي عالج جريمة الدخول والبقاء غير المصرح بهما، فإن الركن المادي فيها يتكون من سلوك إجرامي يتخذ صورة الدخول بنية الغش إلى منظومة المعلومات ونظم معالجتها، كما يمكن أن يتحقق إلى جانبه سلوك آخر يتمثل في فعل البقاء داخل النظام.

- ويتضح لنا أن هدف المشرع هو حماية نظام المعالجة الآلية للمعطيات بصورة مباشرة أو غير مباشرة، وأيضاً حماية المعطيات والبيانات الموجودة داخله، سواء من خلال الدخول أو البقاء غير المسموح به، وحسناً فعل المشرع وهذا نظراً للقيمة المستحدثة للمعلومات المخزنة آلياً.

(2) الركن المعنوي للجريمة:

- جريمة الدخول أو البقاء داخل النظام المعلوماتي جريمة عمدية يتخذ الركن المعنوي فيها صورة القصد الجنائي بعنصريه (العلم والإرادة) بحيث أن القصد الجنائي يثبت إلى المتهم كلما توفر فيه عنصر الغش طالما أنه تعمد إتيان هذا الفعل وبدون ترخيص من صاحب النظام.

(3) المشروع في الجريمة :

- يلاحظ أن المشرع لم يكتفي بتجريم فعل الدخول أو البقاء غير المصرح بهما في النظام المعلوماتي، بل تجاوز ذلك إلى تجريم مجرد المحاولة أي الشروع في ذلك وهذا ما جاء في عبارة : « ... أو يحاول ذلك »

وهو ما يفيد منه على خطورة هذا الفعل، وأن مجرد المحاولة لا ترتكابه يعد جريمة لها نفس عقوبة الجريمة التامة.

(4) العقوبة المقررة :

- أ) في حالة الجريمة البسيطة :

- إن الصورة البسيطة لهذه الجريمة قرر لها المشرع حسب الفقرة الأولى من المادة 394 مكرر وهي : من ثلاثة (3) أشهر إلى سنة (1) حبس والغرامة المالية من 50,000 دج إلى 200,000 دج

- ب) في حالة الجريمة المشددة :

- هنا شدد المشرع في العقوبة وجعلها مضاعفة وهذا بنص الفقرتين الثانية والثالثة من نص المادة 394 مكرر، بحيث يتضح أن المشرع على حماية النظام المعلوماتي لم يتوقف عن تجريم الدخول إليه أو البقاء فيه، بل يتعداه إلى مواجهة ما هو أخطر منهما وهو :

* إما حذف البيانات أو المعطيات أو تغييرها
* إما تخريب نظام إشتغال المنظومة

- بحيث تضاعف العقوبة وتشدد في هاذين الحالتين إلى الحبس من ستة (6) أشهر إلى سنتين (2) والغرامة المالية من 50,000 دج إلى 300,000 دج.

ثانياً: جريمة التلاعب في معطيات نظام المعالجة الآلية للمعطيات:

= هذه الجريمة نصت عليها المادة 394 مكرر 1 من قانون العقوبات بقولها: «يعاقب بالحبس من ستة (6) أشهر إلى ثلاث (3) سنوات وغرامة مالية من 500,000 دج إلى 4.000.000 دج، كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها».

* يبدو أن المشرع الجزائري ولكي يعطي مفهوماً أوسع لفكرة الحماية الجنائية للمنظومة المعلوماتية ولحرمة الحياة الخاصة للأفراد أو للمؤسسات، قام بوضع سياج قانوني متكامل، من خلال تصور السلوكيات التي قد تترتب عن الدخول غير المشروع من أفعال قد يقدم عليها الجناة من إدخال أو إزالة أو تعديل للمعطيات التي يتضمنها النظام بطريق الغش، سواء كان هذا المساس عن عمد أو عن غير عمد.

① الركن المادي للجريمة :

- النشاط الإجرامي في هذه الجريمة ينحصر في أفعال (الإدخال - الإزالة - التعديل) ويكفي توافر إحداها لقيام الجريمة، فلا يشترط إجتماعها معاً حتى يتوافر النشاط الإجرامي فيها، لكن القاسم المشترك في هذه الأفعال الثلاثة هو إنطواؤها على التلاعب بالمعطيات المخزنة والمعالجة داخل النظام.
- وبناءً عليه فالجريمة لا تتحقق إذا وقع النشاط الإجرامي على المعطيات الموجودة خارج النظام سواء قبل دخولها أو بعد خروجها منه، وإنما تأخذ وصف تجريمي آخر.

② الركن المعنوي للجريمة :

الركن المعنوي:2

وهو الحالة النفسية للجاني (أي العلاقة التي تربط بينما ماديات الجريمة وشخصية الجاني) و الذي سيدرس يقوم على مبدأ الإرادة و مبدأ العلم، فهو يستخدم الإرادة الواعية في هذا النوع من الإجرام، فالمجرم يتحكم عليه بخطورة الواقعة و لو كان يجهل العقوبة التي جرمها، وعليه يقوم القصد الجنائي مباشرة وقرينة ذلك النتيجة، ودرس كيف يتم إثبات ذلك؟

- يتم إثبات ذلك بمجرد الدخول غير المصرح به و هو العلم (بالحظر)

لذا لفت ذهن القضاء الفرنسي الى القول أن مخالفة سوء النية هو الأهم في جرائم الانترنت