# 3- جريمة الاحتيال الإلكتروني

د.ملاك عرب دعكور

تاريخ الاستلام: 2/1/2020 تاريخ القبول: 1/2/2020

**المقدمة**

شهد العقدان الاخيران تطورا سريعا ومذهلا في مجال تكنولوجيا المعلومات والاتصالات خاصة مع ظهور شبكة الإنترنت بحيث اصبحت تشكل عالماً افتراضياً يشمل المعاملات المالية والتجارية والمصرفية وغيرها الى ان وصل الامر لظهور الحكومة الإلكترونية، سبق هذا التطور السريع والمذهل كل التوقعات وساهم بشكل ايجابي في تطور حياة الانسان الا انه في الوقت نفسه وككل مجال مستحدث يحتاج الى صياغة قوانين وانظمة لحماية الحقوق في هذا العالم الافتراضي الواسع لاسيما في مجال حماية الحقوق من التعديات والجرائم المالية التي توسلت الشبكة العنكبوتية (الإنترنت) للاستيلاء على الاموال والتي سميت اصطلاحاً بالجرائم الإلكترونية التي لم تطلها وتلحظها القوانين المصاغة قبل ظهور هذا التطور ولكي لا يبقى مرتكبو تلك التعديات بمنأى عن العقاب بسبب فقدان الرادع القانوني بحقهم، كانت الحاجة لتطوير مفهوم الجرائم العادية لتطال الافعال الجرمية المرتكبة بالوسائل الإلكترونية.

ويعتبر من بين التعديات المستحدثة التي هي وليدة التطور التكنولوجي الاحتيال الاكتروني الذي اختير كموضوع لبحثنا. تحول الاحتيال الإلكتروني الى ظاهرة جديدة اتاحت لمرتكبيها الوصول الى الضحايا بسهولة بالغة خاصة مع انتشار الإنترنت كوسيلة مهمة لتقديم الخدمات المالية والمصرفية. ونظرا لأن هذه الجريمة باتت كثيرة الوقوع في مجتمعاتنا وللحد من ارتكابها، سنقوم بدراسة ماهية جريمة الاحتيال الإلكتروني وما اذا كان يمكن ادراج هذا الشكل المستحدث من الاحتيال ضمن اطار الاحتيال العادي المنصوص عنه في نص المادة 655 ق.ع وذلك من خلال تبيان الاساليب الحديثة التي يمكن ان تكون وسيلة لإتمام فعل الاحتيال اضافة الى البحث في الجوانب الموضوعية والاجرائية لهذه الجريمة مع محاولة لتقديم الحلول القانونية لمكافحتها. كذلك سنعمد الى معالجة كيفية مكافحة هذا النوع من الجرائم من خلال تبيان مسؤولية مرتكبيها وكيفية ضبطها واثباتها ولجهة الاختصاص القضائي في ظل الطابع العابر للحدود ولجهة التعاون بين الدول لملاحقة هذا النوع من الجرائم.

بناء عليه، سنقوم بتقسيم بحثنا هذا الى فصلين حيث نتناول في الفصل الأول الطابع الموضوعي لجريمة الاحتيال الإلكتروني على ان يخصص الفصل الثاني لدراسة الطابع الاجرائي لجريمة الاحتيال الإلكتروني.

**الفصل الأول**

**الطابع الموضوعي لجريمة الاحتيال الإلكتروني**

تتمتع كل جريمة بطابع موضوعي يتعلق بالشروط والآثار الموضوعة لها، فجريمة الاحتيال الإلكتروني يتكون طابعها الموضوعي من ركنها المادي المتمثل بالفعل الجرمي أي المناورات الاحتيالية ومن النتيجة الجريمة المستدل عليها من خلال تسليم المال موضوع جريمة الاحتيال ومن ركنها المعنوي أي النية الجرمية حيث تمتاز هذه الجريمة بوجود محاولة لارتكابها.

فقد نصت المادة 655 ق.ع. على أنه كل من حمل الغير بالمناورات الاحتيالية على تسليمه مالاً منقولاً أو غير منقول أو أسناداً تتضمن تعهداً أو إبراء أو منفعة واستولى عليها يعاقب بالحبس من ستة

أشهر إلى ثلاث سنوات وبالغرامة من مئة ألف إلى مليون ليرة.

وتعتبر من المناورات الاحتيالية:

1 – الأعمال التي من شأنها إيهام المجني عليه بوجود مشروع وهمي أو التي تخلق في ذهنه أملاً بربح أو تخوفاً من ضرر.

2 – تلفيق أكذوبة يصدقها المجني عليه نتيجة تأييد شخص ثالث ولو عن حسن نية أو نتيجة ظرف مهد له المجرم أو ظرف استفاد منه.

3 – التصرف بأموال منقولة أو غير منقولة ممن ليس له حق أو صفة للتصرف بها أو ممن له حق أو صفة للتصرف فأساء استعمال حقه توسلاً لابتزاز المال.

4 – استعمال اسم مستعار أو صفة كاذبة للمخادعة والتأثير، ويطبق العقاب نفسه في محاولة ارتكاب هذا الجرم.

وقد أشار قانون العقوبات الفرنسي في نص المادة 313–1[442] منه إلى أن الاحتيال هو عملية إيقاع شخص طبيعي أم معنوي بالغلط عبر استعمال اسم مستعار أو صفة كاذبة وإما بإساءة استعمال صفة حقيقية وإما باستخدام وسائل احتيالية يقوم المجني عليه على أثرها بتسليم أموال أو أوراق مالية أو أي ممتلكات أو يقوم بتوفير خدمة أو الموافقة على عمل أو التزام أو بإعطاء إبراء.

وعليه، سنقوم بتقسيم هذا الفصل إلى مبحثين بحيث يخصص المبحث الأول لدراسة الركن المادي لجريمة الاحتيال الإلكتروني على أن نتناول في المبحث الثاني منه الركن المعنوي لهذه الجريمة.

**المبحث الأول: الركن المادي لجريمة الاحتيال الإلكتروني**

يقسم الركن المادي لجريمة الاحتيال الإلكتروني ككل جريمة إلى فعل مادي يتمثل بالمناورات الاحتيالية (المطلب الأول) التي قد تختلف بين الاحتيال العادي والاحتيال الإلكتروني وإلى نتيجة جرمية تتمثل بتسليم المال (المطلب الثاني) نتيجة تلك المناورات الاحتيالية.

**المطلب الأول: الفعل المادي المتمثل بالمناورات الاحتيالية**

وفق المادة 655 ق.ع. السالفة الذكر، فإن الشروط المطلوب توافرها في موضوع الاحتيال هي أن يكون موضوع الاحتيال مالاً مادياً سواء أكان هذا المال منقولاً أم عقاراً وأن يكون هذا المال مملوكاً للغير. إن الاحتيال جريمة تتضمن الاعتداء على حق الملكية ولا يصلح للملكية إلا الشيء الذي له صفة المال. ويقصد بالمال، كل شيء يصلح محلاً لحق عيني، وعلى وجه التحديد حق الملكية، والأصل أن كل شيء نافع للإنسان يصلح لأن يكون هدفاً للاستئثار وإنشاء الحقوق عليه، ولا يخرج عن هذا الأصل إلا الأشياء التي لا تقبل بطبيعتها أن تكون محلاً لحق عيني كالإنسان. كما يخرج عن مفهوم المال الأشياء التي لا يستطيع أحد أن يستأثر بحيازتها كالمياه في البحار وإذا كان الشيء يصلح بطبيعته محلاً لحق عيني فهو مال حتى لو كان القانون يحظر التعامل فيه كالمخدرات أو الأسلحة الممنوعة[443].

ويشترط في المال أن يكون ذا طبيعة مادية أي قابلاً للحيازة والتسليم والتملك ويخرج عن مفهوم

(442) Pénal: L'escroquerie est le fait soit par l'usage d'un faux nom ou d'une fausse qualité, soit par l'abus d'une qualité vraie, soit par l'emploi de manœuvres Frauduleux, de tromper une personne, physique ou morale et le la déterminer ainsi, à son préjudice ou au= =préjudice d'un tiers, à remettre des fonds des valeurs ou un bien quelconque, à fournir un service ou à consentir un acte opérant obligation ou décharge.

(443) محمود نجيب حسني، جرائم الاعتداء على الأموال في قانون العقوبات اللبناني، دراسة مقارنة، دار النهضة العربية، بيروت، 1984، ص 384.

المال، الأشياء المعنوية كالأفكار والآراء لأنها أشياء لا تدرك بالحس وليس لها كيان مادي يمكن الاستيلاء عليه. لكن هذه الأشياء تتحول إلى مال مادي إذا أفرغت في وعاء مادي كالسند أو الكتاب أو براءة الاختراع، فالاستيلاء على هذه الأشياء بالخداع يتحقق فيه جرم الاحتيال [444] ومتى اكتسب الشيء صفة المال فإنه يصلح أن يكون موضوعاً للاحتيال.

هذا ويتضح لنا أنه عندما يكون محل التسليم شيئاً له صفة المال المادي كالنقود أو المنقولات أو العقارات أو الأسناد التي تتضمن تعهداً أو إبراء فيصلح عنها بأن يكون موضوع جريمة الاحتيال الإلكتروني. والإشكالية تكمن فيما إذا كان ينطبق وصف المال المادي على المعلومات أو البرامج؟ بمعنى إذا قام الفاعل بالدخول إلى أحد المواقع التي تبيع البرامج عبر الإنترنت واستخدم بطاقة ائتمان مزورة في عملية الدفع الإلكتروني واستلم البرنامج المعلوماتي عن طريق تحميله مباشرة عبر الإنترنت، فهل يعد ذلك احتيالاً؟

تباينت الآراء حول هذا التساؤل إلا أننا نؤيد أصحاب الرأي الذي يعتبر الشيء مالاً بالنظر إلى قيمته الاقتصادية لا بالنظر إلى ما له من كيان مادي معتبرين أن القانون يعد منفصلاً عن الواقع إذا لم يسبغ صفة المال على الأشياء ذات القيمة الاقتصادية ومن ثم يمكن إعطاء صفة المال لبرامج وبيانات ومعلومات الحاسوب على أساس ما لها من قيمة اقتصادية، لذلك لا بد من شمولها بالحماية الجزائية[445].وبما أنه يمكن إعطاء صفة المال للبرامج والمعلومات، فهذا يعني أن هذه الأخيرة تصلح لأن تكون محلاً للملكية إذ إن قاعدة «الحيازة في المنقول سند الملكية تنطبق على المعلومات والبرامج فضلا عن أن البرنامج هو ملك لمن ابتكره وفقاً لقوانين حماية الملكية الفكرية لذلك فالمعلومات أو البرامج تصلح لأن تكون محلاً لملكية الغير التي يمكن أن تقع عليها جريمة الاحتيال»[446].

وبالنسبة إلى طبيعة البرامج والمعلومات فهي من المنقولات لأنه عند تشغيل الحاسوب تنتقل هذه المعلومات من ذاكرة الحاسوب إلى الشاشة، ثم إلى ذهن المتلقي وهي عبارة عن إشارات إلكترونية تشبه التيار الكهربائي القابل للانتقال، على الرغم من عدم حيازته المادية[447].

هذا وقد عددت المادة 655 ق.ع. الوسائل الاحتيالية بحيث سنقوم بتبيانها تباعاً.

**1 – الأعمال التي من شأنها إيهام المجني عليه بوجود مشروع وهمي أو التي تخلق في ذهنه أملاً بربح أو تخوفاً من ضرر.**

كمن يرسل عبر البريد الإلكتروني طلباً إلى صاحب البريد بإعادة إرسال كلمة السر العائدة لحسابه المصرفي بحجة تجديد الحسابات لدى المصرف أو إعادة تنظيمها فيقوم العميل بإرسال رقمه السري للمرسل الذي لا يمت بصلة للمصرف.

والسؤال الذي يطرح، هل يعتبر الاستحصال على بطاقة الائتمان أو رقمها السري من قبيل السرقة أم الاحتيال؟

وفق نص المادة 635 ق.ع تحصل السرقة دون وقوع المجني عليه بالغلط بينما يشترط للاعتداد بجريمة الاحتيال وقوع المجني عليه بالغلط المؤدي إلى تسليم المال نتيجة المناورات الاحتيالية، فجريمة

---

(444) علي عبد القادر القهوجي، قانون العقوبات القسم الخاص، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2001، ص 665.

(445) ) (Pierre Catala, Informatique et droit pénal, Travaux de l'institut de sciences criminelles de Poitiers, édition Cujas, 1983, P. 267.

عفيفي كامل عفيفي، جرائم الكومبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، منشورات الحلبي الحقوقية، بيروت، 2003، ص 13.

(446) هدى حامد قشقوشي، جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية، القاهرة، ص 58.

(447) المرجع نفسه، ص 56.

الاحتيال تشترط في عناصرها الأساسية تسليم الشيء بعلم المالك بينما في السرقة يؤخذ الشيء «خفية أو عنوة» أي دون معرفة المالك فضلاً عن أن الاعتداء في جرم الاحتيال ينال من الملكية المنقولة والعقارية على السواء في حين أنه يقتصر على الملكية المنقولة في السرقة.

وقد قضي في هذا الإطار أن الاستحصال على بطاقة الائتمان بواسطة المناورات الاحتيالية التي توقع المجني عليه بالغلط المؤدي إلى تسليم بطاقة الائتمان أو استخدام المناورات الاحتيالية لاستعمال بطاقة ائتمان لا تعود للفاعل أو استخدام المناورات الاحتيالية للتمكن من معرفة الرقم السري يشكل جرم الاحتيال(448). هذا من ناحية، ومن ناحية أخرى، قضي أن أخذ بطاقة الائتمان هو سرقة من ثم دفع ثمن مشتريات أو سحب الأموال بواسطتها يعتبر احتيالاً، وبالتالي يلاحق الفاعل بجريمة السرقة والاحتيال(449).

**2 – تلفيق أكذوبة يصدقها المجني عليه نتيجة تأييد شخص ثالث ولو عن حسن نية أو نتيجة ظرف مهد له المجرم أو ظرف استفاد منه.**

وفق هذه الحالة، لا تكفي الأكذوبة وحدها للاعتداد بها كمناورة احتيالية بل يجب أن يتم تصديقها من قبل المجني عليه نتيجة لتأييد شخص ثالث حسن النية كان أم سيئاً وإما نتيجة ظرف مهد له الفاعل أو استفاد منه(450). وقد نلحظ هذا النوع من المناورات عبر شركة الإنترنت حيث يستوهم مستخدم الإنترنت وجود مشروع معين مغرٍ نتيجة لتأييد بعض الأشخاص الوهميين الذين علقوا على الموقع الإلكتروني أو نتيجة مرورهم عن طريق إحدى وسائل التواصل الاجتماعي وتعليقهم على الموضوع مما أوقع المجني عليه بالغلط وجعله يسلم المال إلى الجاني.

**3 – التصرف بأموال منقولة أو غير منقولة ممن ليس له حق أو صفة للتصرف بها أو ممن له حق أو صفة للتصرف فأساء استعمال حقه توسلاً لابتزاز المال**

وقد نشهد هذه المناورة في الاحتيال الإلكتروني عندما يقوم شخص ببيع موقعاً إلكترونياً لا يملكه عبر الشبكة الرقمية، أن يتلقى بدل البيع على أساس أنه المالك في حين أنه فعلياً لا يقع بالصفة التي تخوله القيام بذلك.

إضافة إلى ذلك، فإنه يوجد عبر الشبكة العنكبوتية العديد من المواقع المتخصصة ببيع المنقولات والعقارات حيث يقوم الباعة بعرض ما يرغبون بيعه عن طريق هذه المواقع. فمثلاً، إذ قام شخص بعرض هاتف خليوي عن طريق أحد هذه المواقع، وقام المشتري بدفع ثمنه من خلال بطاقة الائتمان إلا أن البائع لم يقم بشحن الهاتف إلى المشتري بل قام ببيعه مرة أخرى.

**4 – استعمال اسم مستعار أو صفة كاذبة للمخادعة والتأثير.**

من يقوم باستعمال بطاقة ائتمان لا تمت له بصلة لسحب النقود أو الوفاء لدى التجار، فإنه يرتكب جرم الاحتيال بوسيلة انتحال صفة كاذبة وهي صفة الحامل الشرعي كما أنه يتخذ اسماً كاذباً وهو اسم الحامل الشرعي(451).

كذلك، لاحظنا أنه يلجأ إلى خداع المستهلك عبر إرساله رسالة يدلي المرسل عبرها أنه شخص

---

(448) CA Versailles,, 6: Ch, 29 Oct. 2013, No. 12/03791, www.legifrance.gouv.fr

(449) CA Paris, 9: Ch, 23 Mai 2013, No. 12/03900, www.legifrance.gouv.fr

(450) Nidal El Chaer, La Criminalité informatique devant la justice pénal, Sader 2004, P. .

من أوهم أباه أنه بإمكانه تأمين إشارات سفر إلى لندن وبعد الاجتماع بالمجني عليهم وتسليم الجاني الأموال وجوازات السفر بناءً على تأكيد قدرة الجاني على تأمين التأشيرات من قبل والده.

محكمة التمييز الجزائية، الغرفة السادسة، قرار رقم 214 تاريخ 19/7/2005، كساندر 2005، ق 1434.

(451) نائلة قورة، مرجع سابق، ص 541.

يتبوأ منصباً معيناً كمدير شركة أو عضو في فريق صيانة بريد الموقع ويطلب معلومات عن حساب المستهلك متذرعاً بحجة ما فيقع المستهلك في الخداع ويستجيب لطلبه[452].

كما نشهد حالة إنشاء مواقع وهمية للبيع والشراء وما إن يدخل مستخدم الإنترنت ويقوم بشراء ما يحتاجه عن طريق وضع أرقام بطاقته الائتمانية لحسم المبالغ النقدية المستحقة مقابل البضاعة حتى يقع في المحظور ولا تصل أي بضاعة بعد أن يكون قد فقد جزءًا من نقوده من خلال بطاقته الائتمانية ويكتشف بأنه كان ضحية لجريمة الاحتيال الإلكتروني[453]. هذا وقد لاحظنا أن كثيراً ما يتم استخدام البنك الدولي في إطار عملية الاحتيال إذ قد يدعي شخص أو منظمة ما أنهما تابعان للبنك الدولي ويطلبان مالاً أو تفاصيل شخصية أو معلومات مصرفية للحصول على وظيفة أو قرض شخصي أو بطاقة صراف آلي/ بطاقة ائتمان.

وهنا تجدر الإشارة إلى أن البنك الدولي لا يرسل هذه الأنواع من الرسائل كما أنه لا يمكن مساعدة أي شخص في استرداد أية أموال مفقودة[454].

**المطلب الثاني: النتيجة الجريمة المتمثلة بتسليم المال**

يكتمل الركن المادي لجريمة الاحتيال بشكل عام عندما يتم تسليم المال نتيجة المناورات الاحتيالية بمعنى أن يتم تسليم المال إلى المحتال نتيجة الغلط الذي وقع فيه جراء الخداع الذي مورس بحقه بفعل المناورات الاحتيالية التي سبق وذكرناها. وقد قضى في هذا الإطار أنه يكفي لتكوين جريمة الاحتيال أن تكون إرادة من تنازل عن الحيازة غير حرة بسبب المناورات الاحتيالية. وأن جوهر جرم الاحتيال يقوم على العبث في الحقائق وإخفائها عن المجني عليه مما يوقعه في غلط يدفعه للتصرف على نحو مضر بمصلحته، مالية كانت أم عقارية، وبحيث أنه ما كان ليقدم عليه، لو كان مدركاً الحقيقة المحجوبة عنه بفعل المحتال ومعاونيه إذا ما وجدوا[455].

هذا وإنه من الواجب لتوافر جرم الاحتيال أن يكون تسليم المال قد تم نتيجة الخداع والمناورات الاحتيالية[456]، وبالتالي لا يمكن اعتبار جريمة الاحتيال واقعة إلا بعد حصول تسليم الشيء موضوع الاحتيال فهو الذي يعتبر العنصر المكمل لها، وبدونه لا يمكن وصف الفعل إلا بالعمل التحضيري أو على الأكثر بمحاولة الاحتيال[457].

وقد قضي أنه لقيام جنحة الاحتيال قانوناً واكتمال أركانها ينبغي أن تسبق المناورات الاحتيالية فعل التسليم بمعنى أنه إذا سلم المجني عليه ماله إلى المدعى عليه من دون أن تصدر من هذا الأخير أفعال غش وخداع عابت إرادته ثم التجأ بعد ذلك إلى المناورات الاحتيالية ليتخلص من الالتزام الناشئ بذمته نتيجة استلامه المال، فإن جريمة الاحتيال لا تتحقق بعناصرها القانونية[458].

بمعنى آخر، تكتمل جريمة الاحتيال من لحظة تسليم المال موضوع الاحتيال إلى المحتال نتيجة المناورات الاحتيالية مما يعني أن تسليم المال حصل نتيجة عيب في إرادة المجني عليه.

وهنا يثار التساؤل عن طبيعة المال المسلم في الاحتيال الإلكتروني؟

---

(452) إيناس شري، الاحتيال عبر الإنترنت.

CA Toulouse, 3: Ch, 30/3/2006 No. 05/01432, Jurisdata 2006-01432.

(453) عبد الفتاح سليمان، الاحتيال في العمل المصرفي في الدول العربية وطرق مكافحتها، منشأة المعارف، الإسكندرية، 2012، ص 47.

(454) http.www.albankaldawli.org/ar/about/unit/integrity-vicepresidancy/report-anallegation.

(455) محكمة التمييز الجزائية، قرار رقم 19 صادر بتاريخ 5/2/2009، صادر في التمييز 2009.

(456) محكمة التمييز الجزائية، الغرفة الثالثة، قرار رقم 226 صادر بتاريخ 1/7/98، كساندر 1998، ص 59.

(457) الهيئة الاتهامية، قرار أساس 130 صادر بتاريخ 1/4/85، العدل 86، ج 4، ص 59.

(458) محكمة التمييز الجزائية، الغرفة السابعة، قرار رقم 55 صادر بتاريخ 26/1/2006، كساندر 2006، ق 98.

لقد سبق وأشرنا إلى أن الشروط المطلوب توافرها في موضوع الاحتيال هي أن يكون موضوع الاحتيال مالاً مادياً سواء أكان هذا المال منقولاً أم غير منقول وأن يكون هذا المال مملوكا للغير.

وأوضحنا أنه إذا كان الشيء موضوع الاحتيال أفكاراً ومعلومات فإنه يعتبر مالاً بالنظر إلى قيمته الاقتصادية لا بالنظر إلى ماله من كيان مادي. فضلاً عن ذلك، فإننا نوضح أن المال المنقول فيما يتعلق بالاحتيال الإلكتروني هو عبارة عن تحويل مبلغ معين من المجني عليه إلى المحتال.

كما يمكن أن يقع الاحتيال الإلكتروني على الأموال غير المنقولة كالعقود الإلكترونية والبرامج الإلكترونية وغيرها من الوسائل المستخدمة من أجل إتمام هذا الجرم والتي تعد وسائل رقمية متطورة تحصل عبر شبكة الإنترنت.

وهنا نلاحظ الفرق بين الاحتيال العادي والإلكتروني إذ إنه في النوع الأول يتم تسليم المال موضوع الاحتيال باليد حتى لو تم التسليم من قبل شخص غير المجني عليه أو أن يتم الاستيلاء من قبل شخص غير المحتال[459]، بينما لاحظنا أنه في الاحتيال الإلكتروني، لا وجود لتسليم فعلي باليد إنما يتم التسليم على شبكة الإنترنت من حساب إلى آخر أو تسليم سند إلكتروني من خلال البريد الإلكتروني أو أي وسيلة أخرى عبر الشبكة العنكبوتية تمكن إرسال السند من المجني عليه إلى المحتال.

هذا فيما يتعلق بالتسليم. أما فيما يتعلق بالمناورات الاحتيالية، فالاعتداد بالاحتيال الإلكتروني يشترط أن تتم المناورات الاحتيالية بوسائل إلكترونية حتى لو حصل التسليم باليد وهذا ما لا يمكن أن نلحظه بالاحتيال العادي إذ إن المناورات لا يمكن أن تحصل عن طريق الوسائل الإلكترونية وإلا نكون أمام احتيال إلكتروني.

هذا وقد يتساءل البعض، هل يتحقق التسليم في حال تلاعب الجاني بالبرامج أو المعلومات المصرفية بهدف تحويل الأموال من حسابات أصحابها إلى حسابه؟

اعتبر القضاء الفرنسي أن الدفع الذي يتم عن طريق القيد الكتابي يعادل تسليم النقود[460].

بناءً عليه، فإن نص المادة 655 ق.ع. ونص المادة 313-1 ق.ع.ف. ينطبقان على جميع أفعال التلاعب في عملية البرمجة أو في البيانات المدخلة إلى الحاسوب والمنقولة عبر الإنترنت.

هذا يعني أن عمليات التحويل الحاصلة عبر شبكة الإنترنت نتيجة التلاعب بأنظمة المصارف والتي ترتب عليها الاستيلاء على كل أو بعض الأرصدة العائدة للغير، يعد التسليم بها محققاً ومعادلاً لتسليم النقود.

## المبحث الثاني: الركن المعنوي لجريمة الاحتيال الإلكتروني

لا يكفي لقيام الجريمة قانوناً أن يقوم الفاعل بارتكاب الفعل المادي فيها وإنما يلزم أيضاً توافر رابطة نفسية بين الفاعل وماديات الجريمة يطلق عليها الركن المعنوي[461].

جريمة الاحتيال هي جريمة قصدية تستلزم نية جرمية أو قصداً جرمياً عند فاعلها، بارتكاب فعل الخداع نتيجة المناورات الاحتيالية للاستيلاء على المال. ويعود تقدير توفر النية الجريمة أو عدمه إلى قضاة الأساس بمعزل عن رقابة محكمة التمييز[462].

تدخل جريمة الاحتيال في عداد الجرائم القصدية حيث يتمثل القصد فيها بعلم الفاعل بأن أفعاله ليس

---

(459) محكمة التمييز الجزائية، الغرفة السادسة، قرار رقم 19 صادر بتاريخ 15/1/2004، صادر في التمييز، القرارات الجزائية، صادر 2004، ص 2.

(460) Cass Crim, 7 Mars 2019, www.legifrance.gouv.fr

(461) Bernard Bouloc, droit penal general, Dalloz, Paris, 2013, P. 241

سمير عاليه، شرح قانون العقوبات (القسم العام) المؤسسة الجامعية للدراسات والنشر والتوزيع، مجد، بيروت، 2002، ص 253.

(462) فيلومين نصر، قانون العقوبات الخاص، المنشورات الحقوقية صادر، بيروت 2013، ص 171.

لها أساس من الصحة وبأنه لا تتوافر له صفة المالك على المال الذي يتصرف فيه بمعنى علم المحتال بأن المال الذي يريد أن يتسلمه هو مال مملوك لغيره وأن تنصرف إرادته إلى ارتكاب فعل الخداع من خلال إحدى المناورات الاحتيالية المنصوص عليها في نص المادة 655 ق.ع. إضافة إلى اتجاه إرادته إلى تحقيق النتيجة الجرمية المتمثلة في حمل المجني عليه على تسليم المال(463).

هذا يعني أن لا جريمة احتيال فيما لو ظن مثلاً الفاعل أن له حقاً بالاسم المستعار أو الصفة الكاذبة أو إذا كان له إيمان راسخ بالمشروع الوهمي(464). كما أنه لا يمكن تصور وقوع جريمة احتيال إلكتروني نتيجة خطأ ناتج عن إهمال أو قلة احتراز أو عدم مراعاة القوانين والأنظمة.

فمن غير المنطقي أن يقوم الفاعل بمراسلة شخص معين والعمل على الاستحصال على كلمة السر لحسابه المصرفي من دون أن يتوافر لديه القصد.

إذاً، القصد الجزائي يتوافر في جريمة الاحتيال العادية والإلكترونية مع فارق أن الغاية في الاحتيال الإلكتروني تتم عبر استخدام شبكة الإنترنت.

والسؤال الذي يطرح، هل يشترط توفر الضرر بحق المجني عليه للاعتداد بجرم الاحتيال؟

لم يرد في نص المادة 655 ق.ع. عبارة حصول الضرر وعملاً بقاعدة مبدأ شرعية الجرائم والعقوبات، فإنه يكتفي بتوافر عناصر جرم الاحتيال التي تؤدي إلى تحقيق النتيجة الجرمية والمتمثلة بتسليم المال. فبرأينا إن الضرر يتحقق بمجرد تسليم المال أي خسارته.

هذا وأنه وفقاً للفقرة الأخيرة من المادة 655 ق.ع.، فإنه يطبق العقاب نفسه في محاولة ارتكاب جرم الاحتيال، وهذا يشكل استثناءً إذ إن المحاولة غير معاقب عليها في الجنح إلا إذا ورد نص صريح بشأنها. ويمكن تصور وقوع محاولة احتيال إلكتروني في حال تراجع المحتال مثلا عن الاستيلاء على مال المجني عليه بعد أن استحصل على الرقم السري لحسابه المصرفي نتيجة المناورات الاحتيالية سواء بعامل شخصي داخلي أم بعامل خارجي.

## الفصل الثاني

## الطابع الإجرائي لجريمة الاحتيال الإلكتروني

بعد التطرق إلى الطابع الموضوعي لجريمة الاحتيال الإلكتروني،لا بد من معالجة الطابع الإجرائي الذي يمكن من تطبيق الطابع الموضوعي من خلال التطرق في المبحث الأول منه تحت عنوان استقصاء جريمة الاحتيال الإلكتروني الى الجهات المختصة داخليا ودوليا لاستقصاء جريمة الاحتيال الإلكتروني وإثباتها كذلك البحث في المبحث الثاني تحت عنوان آلية مكافحة جريمة الاحتيال الإلكتروني في ماهية المحكمة المختصة للنظر في الدعاوى الناشئة عن جريمة الاحتيال الإلكتروني فضلا عن تسليط الضوء على التعاون الدولي لضبط هذه الجريمة.

### المبحث الأول:استقصاء جرائم الاحتيال الإلكتروني:

لما كان الطابع التقني يغلب على الجرائم المعلوماتية مع ما يتطلب ذلك من خبرات فنية متخصصة لكشفها وجمع الأدلة حولها، كان لا بد من إنشاء وحدات متخصصة في قوى الأمن للتحقيق فيها، لذلك أنشئ مكتب مكافحة جرائم المعلوماتية في لبنان، كما أنشئت مكاتب متخصصة بجرائم المعلوماتية

(463) محكمة التمييز الجزائية، الغرفة السادسة، قرار رقم 14 صادر بتاريخ 23/1/2001، المصنف في القضايا الجزائية، للدكتور عفيف شمس الدين، 2001، ص 259.

(464) http.www.belgium.be/fr/justice/securite/criminalite/criminaliteinfromatique/fraude) informatique.

تاريخ زيارة الموقع 4/8/2019

على الصعيد الدولي(المطلب الأول). فضلا عن ذلك، فإنه لا بد من إلقاء الضوء على مسألة إثبات ارتكاب جريمة الاحتيال الإلكتروني (المطلب الثاني).

**المطلب الأول: المكاتب المعنية في جرائم المعلوماتية**

سوف نتناول في هذا المطلب المكتب المعني على الصعيد الوطني بجرائم المعلوماتية حيث تدخل جريمة الاحتيال الإلكتروني في عدادها (الفرع الأول) ونخصص المطلب الثاني لإلقاء نظرة على المكاتب المعنية بجرائم المعلوماتية على الصعيد الدولي (الفرع الثاني).

**الفرع الأول: مكتب مكافحة جرائم المعلوماتبة والملكية الفكرية في لبنان**

أنشئ مكتب مكافحة جرائم المعلوماتية وحماية الملكية الفكرية التابع لقسم المباحث الجنائية الخاصة ضمن وحدة الشرطة القضائية في المديرية العامة لقوى الأمن الداخلي، بموجب مذكرة الخدمة رقم 609/204 تاريخ 8/3/2006 وهو يعنى بمكافحة الجرائم التي تستخدم فيها التقنيات المعلوماتية وجرائم التعدي على الملكية الفكرية. يتمتع هذا المكتب بصلاحيات مكافحة الجرائم على الأراضي اللبنانية، ويتحرك تلقائياً في حال الجرم المشهود وفقاً لمعلومات خاصة لديه بعد أخذ إشارة النيابة العامة المختصة. يوزع عناصر المكتب بين إدارة وتقنية ومحققين.

تجدر الإشارة إلى أن عناصر هذا المكتب قد تابعوا دورات تقنية عدة في مجال مكافحة جرائم المعلوماتية وحماية الملكية الفكرية في معاهد متخصصة تحت إشراف اختصاصيين فنيين عسكريين. كما تم تجهيز المكتب بتجهيزات تقنية متخصصة في كشف الأدلة الجرمية المعلوماتية داخلة الأجهزة المعلوماتية على اختلاف أنواعها وعلى شبكة الإنترنت(465).

**الفرع الثاني: المكاتب المعنية بجرائم المعلوماتية على الصعيد الدولي:**

مع تمييز الجريمة بالعالمية وبكونها عابرة للحدود، لا تحقق مكافحتها إلا بوجود تعاون دولي على المستوى الإجرائي الجزائي بحيث يسمح بالاتصال المباشر بين أجهزة الشرطة في الدول المختلفة وذلك بإنشاء مكاتب متخصصة لجمع المعلومات عن مرتكبي الجرائم المتعلقة بالإنترنت وتعميمها.

**اولا:منظمة الشرطة الجنائية الدولية International Criminal Police Organization**

الإنتربول اختصار لكلمة الشرطة الدولية International Police وهو أكبر منظمة شرطة دولية. أنشئت هذه المنظمة عام 1923 ومكونة من قوات الشرطة لـ 194 دولة ومقرها الرئيسي في مدينة ليون. وقد انتسب إليها لبنان عام 1949.

يتبادل أعضاء الشرطة الدولية المعلومات عن المجرمين الدوليين ويتعاونون فيما بينهم في مكافحة الجرائم الدولية مثل جرائم التزييف والتهريب وعمليات الشراء والبيع غير المشروعة للأسلحة. ويحتفظ أفراد المنظمة بسجلات الجرائم الدولية ويساعدون الأعضاء في النواحي العملية ويقومون بتدريب وعمل استشارات لأفراد الشرطة(466).

**ثانيا:المركز الأوروبي لمكافحة الجريمة الإلكترونية**

تم إنشاء مكتب متخصص بجرائم المعلومات يدعى «المركز الأوروبي لمكافحة الجرائم المعلوماتية» بقرار صادر عن المجلس الأوروبي حيث باشر أعماله في شهر كانون الثاني من العام 2013. اتخذ هذا المركز من هولندا مقراً له. وهو مكلف بمعالجة الجرائم الخطرة والمنظمة على الإنترنت.

(465) لمحة عن مكتب مكافحة الجرائم المعلوماتية وحماية الملكية الفكرية في لبنان: http://www.ucipliban.org/arbicphp?o9ption=com تاريخ زيارة الموقع 13-8-2019

(466) www.interpol.int/ar/3/3 تاريخ زيارة الموقع 13/9/2019

هذا وقد وضع المركز الأوروبي لمكافحة الجريمة الإلكترونية والذي يمول من قبل وكالة الشرطة الأوروبية Europol مجموعة من الأهداف يقوم التركيز عليها وهي الاحتيال عبر الإنترنت وحماية المعلومات الشخصية التي تضمها المواقع الاجتماعية ومكافحة عمليات القرصنة وما ينتج عنها من سرقات للهوية واستعمالها لأغراض إجرامية على الإنترنت، إضافة إلى الاهتمام بملف الاستغلال الجنسي للأطفال عبر الإنترنت والهجمات الإلكترونية التي تؤثر على البيئة الحيوية ونظم المعلومات في الاتحاد الأوروبين وذلك في صدارة اهتمامات المركز.[467].

**ثالثا:مكتب التحقيقات الفدرالي Federal Bureau of Investigation (FBI):**

يعتبر مكتب التحقيقات الفدرالي وكالة حكومية تابعة لوزارة العدل الأميركية وتعمل كوكالة استخبارات داخلية وقوة لتطبيق القانون في الدولة. يتكون مكتب التحقيقات الفدرالي من ستة فروع وظيفية بالإضافة إلى المكتب الرئيسي أو مكتب المدير التنفيذي الذي يتم فيه التحكم بجميع العمليات الإدارية المتعلقة بالوكالة[468].ويقدم المسؤولون في كل فرع التقارير إلى نائب المدير التنفيذي، وترفع التقارير لاحقاً إلى المدير المشارك.

**رابعا:المكتب المركزي لمكافحة الجريمة المتصلة بتكنولوجيا المعلومات والاتصالات**

أنشأ المرسوم رقم 405/2000 بتاريخ 15 أيار 2000 داخل الإدارة المركزية للشرطة القضائية الفرنسية قسماً خاصاً بمحاربة الجريمة الإلكترونية ويعرف بـ «المكتب المركزي لمكافحة الجريمة المتصلة بتكنولوجيا المعلومات والاتصالات.

يعنى المكتب المركزي لمكافحة الجريمة المتصلة بتكنولوجيا المعلومات والاتصالات، بالاعتداءات الواقعة على نظم المعالجة الآلية للبيانات بالاحتيال الحاصل عبر شبكة الاتصالات وبطاقات الائتمان فضلاً عن مختلف أشكال الجريمة الواقعة عبر استخدام التقنيات الجديدة للتكنولوجيا.

**المطلب الثاني: إثبات جريمة الاحتيال الإلكتروني:**

لم يأت قانون أصول المحاكمات الجزائية اللبناني على ذكر الإثبات الإلكتروني، إلا أن القانون رقم 81 الصادر بتاريخ 10/10/2018 تحت عنوان قانون المعاملات الإلكترونية والبيانات ذات الطابع الشخصي تناول مسألة الإثبات في نصوص متفرقة.

**الفرع الأول: الإثبات الخطي**

يمكن تقسيم الوثائق الخطية التي تستعمل كأدلة إثبات عند حصول جريمة معينة إلى: المحاضر– أوراق الجريمة– الأوراق الخاصة. ولكن لا يمكن اعتبار هذه الوثائق ضمن فئة الإثبات الخطي في جرائم المعلوماتية وخاصة في جريمة الاحتيال الإلكتروني.

أشار قانون المعاملات الإلكترونية والبيانات ذات الطابع الشخصي إلى السند الإلكتروني والتوقيع الإلكتروني كوسائل إثبات. فقد نصت المادة 7 منه على أنه يقبل السند الإلكتروني في الإثبات وتكون له ذات المرتبة والقوة الثبوتية التي يتمتع بها السند الخطي المدون على الورق شرط أن يكون ممكناً تحديد الشخص الصادر عنه وأن ينظم بطريقة تضمن سلامته.

كما نصت المادة 9 من ذات القانون على أنه يصدر التوقيع الإلكتروني عن طريق استعمال وسيلة آمنة تعرف عن الموقع وتشكل ضمانة على علاقة التوقيع بالعمل القانوني الذي يرتبط به.

---

(467) https://aitnews.com/2013/01/10 افتتاح-مركز-أوروبي-لمكافحة-الجريمة- الإلكترونية تاريخ زيارة الموقع 17/9/2019

(468) www.Fbi.gov/about-us تاريخ زيارة الموقع https:/ar.wikipedia.org/wiki/مكتب-التحقيات-الفيدرالي-15-9-2019

هذا ولا يزال مفهوم السند الإلكتروني مفهوماً غامضاً غير محدد بشكل ثابت وأكيد حيث اعتبر أن السند الإلكتروني هو مفهوم طارئ على النظام القانوني النافذ حالياً إذ يصعب تكييفه كسند كتابي واعتبار مضمونه كتابه فهذا المضمون لا يظهر إلا باستعمال أجهزة إلكترونية لقراءته[469].

هذا ويأخذ التوقيع الإلكتروني عدة أشكال تتمثل بالرقمي والبيومتري والتوقيع بالقلم الإلكتروني.

يعتمد التوقيع البيومتري على الصفات المميزة للإنسان كبصمة الأصبع وبصمة الصوت وشبكة العين والتعرف على الوجه البشري وسواها من الصفات السلوكية والجسدية.

أما التوقيع بالقلم الإلكتروني فيتم بقلم يمكنه الكتابة على شاشة الحاسوب عن طريق برنامج معلوماتي يتيح التقاط التوقيع والتحقيق من صحته.

بالنسبة للتوقيع الرقمي فهو يعتمد على استخدام اللوغاريتمات بتحويل المحرر المكتوب من نمط الكتابة العادية إلى معادلة رياضية وتحويل التوقيع إلى أرقام بحيث يحفظ جهاز الحاسوب الرقمي بطريقة لا يستطيع أحد معها أن يعيد المحرر إلى صيغته المقروءة إلا الشخص الذي لديه المعادلة الخاصة بذلك والتي تقوم بدور المفتاح[470].

**الفرع الثاني: الخبرة**

من طرق الإثبات المتبعة أمام القضاء الجزائي الخبرة. والمقصود بها الاستعانة بشخص صاحب كفاءة فنية علمية لإعطاء رأيه في مجال اختصاصه ومع تقدم الاكتشافات العلمية والفنية، تقدمت الخبرة في المجال القانوني[471]. هذا ويعود للقاضي في دعاوى جرائم المعلوماتية الحق في تعيين الخبراء المتخصصين في المجال المعلوماتي انطلاقاً من نص المادة 34 أ.م.ج. التي نصت على أنه إذا استلزمت طبيعة الجريمة أو آثارها الاستعانة بخبير أو أكثر لجلاء بعض المسائل التقنية أو الفنية فيعين النائب العام الخبير المختص ويحدد مهمته بدقة.

**أ- العنوان الرقمي IP:**

يعتبر من الأدلة المعلوماتية التي تساهم في حل قضايا الاحتيال الإلكتروني والذي يحتاج إلى خبراء مختصين لتحديد الاحتيال الإلكتروني والكشف عنه. وبمقتضى بروتوكول الإنترنت الذي يختص بعنونة البيانات في الشبكة، يتم التعرف على الحاسبات الآلية الموصولة بشبكة الإنترنت من خلال عناوين عددية حيث لكل حاسب آلي موصول بها عنوانه الوحيد الخاص به تماماً كالحاجة إلى معرفة عنوان المرسل والمرسل إليه من أجل تبادل الرسائل في البريد العادي[472].

**ج- داتا الاتصالات Traffic Data:**

هي وسيلة تخول المحققين التنصت على اتصالات المحتال حيث يستطيعون معرفة مكان وجود أو معرفة هويته الحقيقية أو إذا ما كان قد انتحل صفة.

فهذه البيانات تحدد مصدر الاتصال الرقمي الذي استعمل لارتكاب الجرم ووجهته والطريق التي سلكه والوقت والتاريخ الذي حصل فيهما الجرم والمدة التي استغرق ارتكابه.

**د- سجل العمليات Log Files:**

(469) وسيم الحجار، الإثبات الإلكتروني، المنشورات الحقوقية، صادر، بيروت، 2002، ص 13.

(470) إلياس ناصيف، العقود الدولية، العقد الإلكتروني في القانون المقارن، منشورات الحلبي الحقوقية، بيروت، 2009، ص 244.

(471) عاطف النقيب، أصول محاكمات جزائية، دراسة مقارنة، المنشورات الحقوقية صادر، بيروت، 1993، ص 368.

(472) طوني ميشال عيسى، التنظيم القانوني لشبكة الإنترنت، ط1، المنشورات الحقوقية صادر، بيروت، 2001، ص 524.

يعمد المحتال عبر الحاسوب للولوج إلى النظام المعلوماتي الخاص بالضحية حيث تسجل الأنشطة المعلوماتية الجارية على الـ Log Files الخاص بالحاسوب.فيلجأ المحققون الى log files من أجل معرفة من اخترق قاعدة المعلومات أو دخل إلى البرنامج وما هي الأفعال التي أجراها (سحب ملفات، تعديل في المعلومات...).

**المبحث الثاني: آلية مكافحة جريمة الاحتيال الإلكتروني**

تعد جريمة الاحتيال الإلكتروني من الجرائم المستحدثة في العصر الحالي بحيث تتطلب مكافحتها البحث عن ماهية المحكمة المختصة للنظر في الدعاوى الناشئة عنها على المستوى الوطني (المطلب الأول) وتبيان كيفية ضمان عدم تكرار هذه الجريمة على المستوى الدولي(المطلب الثاني) .

**المطلب الأول: على المستوى الوطني**

تتميز جريمة الاحتيال الإلكتروني بأنها جريمة عابرة الحدود، والإشكالية التي تثار تبعاً لذلك تتمثل في ماهية المحكمة المختصة للنظر في الدعوى الجزائية المتعلقة بالاحتيال الإلكتروني وما هو القانون الواجب التطبيق. نصت المادة 9 أ.م.ج. المتعلقة بالاختصاص المكاني الداخلي على أنه تقام الدعوى العامة أمام المرجع الجزائي الذي وقعت الجريمة ضمن نطاق دائرته أو التابع له محل إقامة المدعى عليه أو محل إلقاء القبض عليه. أما الاختصاص الدولي للمحاكم الجزائية اللبنانية فإنه يحدد وفقاً للصلاحيات المنصوص عنها في قانون العقوبات والتي تشمل الصلاحيات الإقليمية(الفرع الأول)، الصلاحية الذاتية(الفرع الثاني)، الصلاحية الشخصية(الفرع الثالث) والصلاحية الشاملة(الفرع الرابع).

**الفرع الأول:الصلاحية الإقليمية**

تعني الصلاحية الإقليمية وفق نص المادة 15 ق.ع وجوب تطبيق قانون العقوبات على كل جريمة تقع داخل إقليم الدولة بغض النظر عن جنسية الجاني وطنياً كان أم أجنبياً وبصرف النظر عن جنسية المجني عليه أجنبياً كان أم وطنياً وسواء أهددت الجريمة مصلحة للوطن أم لدولة أجنبية[473]. وعليه، فإن ارتكاب أي فعل من أفعال جريمة الاحتيال الإلكتروني في لبنان يجعل المحاكم اللبنانية مختصة للنظر في الدعوى الناشئة عن هذا الجرم وفقاً للصلاحية الإقليمية وذلك كمن يرتكب إحدى المناورات الاحتيالية في لبنان أو إذا كان الجاني أو المجني عليه في لبنان أو من يقوم بالمناورات الاحتيالية في الخارج ويتم تسليم المال عبر حاسوب في لبنان.

**الفرع الثاني:الصلاحية الذاتية**

وفقاً لنص المادة 19 ق.ع. فإنه يجب تطبيق قانون العقوبات اللبناني على الجرائم التي تقع في الخارج وتمس المصالح الأساسية للدولة اللبنانية سواء كان الجاني لبنانياً أم أجنبياً[474].

بناءً عليه، إذا كانت جريمة الاحتيال من شأنها أن تخل بأمن الدولة أو من شأنها ارتكاب إحدى الجرائم المحددة في نص المادة 19 ق.ع. تسهيلاً للقيام بالاحتيال الإلكتروني، تكون المحاكم اللبنانية الجزائية هي المختصة وفقاً للصلاحية الذاتية.

**الفرع الثالث:الصلاحية الشخصية:**

تنعقد الصلاحية الشخصية للمحاكم اللبنانية حسب نص المادة 20 ق.ع عند ارتكاب جريمة احتيال إلكتروني من شخص لبناني خارج الأراضي اللبنانية. هذا وسنداً للمادة 21 ق.ع.، إذا ارتكب الاحتيال الإلكتروني من قبل دبلوماسي أو قنصل أو أي موظف لبناني في الخارج أثناء أو بمعرض ممارستهم لوظيفتهم، تنعقد الصلاحية الشخصية للمحاكم اللبنانية.

---

(473) سمير عاليه، مرجع سابق، ص 118.

(474) علي عبد القادر القهوجي، شرح قانون العقوبات العام، منشورات الحلبي الحقوقية، بيروت 2008 ص 160.

بمعنى آخر، إذا ارتكبت الجريمة من قبل هؤلاء خارج إطار ممارستهم لوظيفتهم، فيتم ملاحقتهم وفق المادة 20 ق.ع. على اعتبار أنهم لا يتمتعون حينها بأي حصانة ويعاملون كأي مواطن يحمل الجنسية اللبنانية.

**الفرع الرابع:الصلاحية الشاملة:**

وفقا لنص المادة 23 ق.ع إذا ارتكب شخص أجنبي أو عديم الجنسية جريمة احتيال إلكتروني خارج الأراضي اللبنانية وتم تواجده في إقليم الدولة اللبنانية، يكون القضاء الجزائي اللبناني هو المختص تبعاً للصلاحية الشاملة طالما لم يرد طلب استرداده أو ورد طلب استرداده إلا أن السلطات اللبنانية قررت رفض هذا الطلب.

**المطلب الثاني:على المستوى الدولي :**

لا يكفي أن نحدد الإطار العام لحماية وضبط هذه الجريمة على المستوى الوطني، بل لا بد من إيجاد إطار شامل يضمن عدم تكرار هذه الجريمة على المستوى الدولي.

لاحظنا من ناحية أنه حتى هذه اللحظة لم يصدر عن الأمم المتحدة أي اتفاقية تعنى بمكافحة الجرائم المعلوماتية بشكل عام. ومن ناحية أخرى، اتضح لنا وجود العديد من الاتفاقيات التي تنبهت للجرائم المعلوماتية بشكل عام ولجريمة الاحتيال الإلكتروني بشكل خاص.

**أولاً: اتفاقية بودابست لمكافحة الجرائم المعلوماتية،** والتي أبرمت بتاريخ 23/11/2001 وهي خاصة لدول الاتحاد الأوروبي. تضمنت هذه الاتفاقية مجموعة من الإجراءات المتعلقة بالتعاون الذي يجري بين الدول الموقعة عليها ومجموعة من المبادئ المرتبطة بعمليات استرداد وتسليم المجرمين المعلوماتيين(475).

**ثانياً: الاتفاقية العربية لمكافحة جرائم تقنية المعلومات،** صدر عن جامعة الدول العربية اتفاقية تعنى بمكافحة الجرائم المعلوماتية سميت بالاتفاقية العربية لمكافحة جرائم تقنية المعلومات حيث وافق على الاتفاقية مجلس وزراء الداخلية العرب بتاريخ 21/12/2010 بعد مصادقة الدول الأطراف عليها(476). هذا وتعد هذه الاتفاقية نقطة تحول في التعاون العربي لمكافحة هذه الجرائم حيث نصت الاتفاقية على التعاون العربي في مكافحة الجرائم المعلوماتية في العديد من المجالات منها التعاون القضائي، تبادل المعلومات، تبادل الخبرات، الاختصاص القضائي، تسليم المجرمين، المساعدة القضائية وغيرها من المواضيع ذات الصلة(477).

تجدر الإشارة إلى أن لبنان لم يصدق على هذه الاتفاقية.

هذا وقد لاحظنا عدم وجود اتفاقيات دولية منظمة لمكافحة الجرائم المعلوماتية بشكل عام على الرغم من وجود بعض الاتفاقيات الدولية في المجال القضائي والتي قد تساعد في مكافحة تلك الجرائم. وسنذكر منها على سبيل المثال:

- التعاون القضائي في المسائل الجزائية بين لبنان وبلغاريا عام 2001.
- الاتفاقية القضائية بين لبنان ومصر عام 1998.
- الاتفاقية العربية للتعاون القضائي بين الدول العربية المعقودة عام 1983 (المعروفة باتفاقية الرياض).

---

(475) www.rm.co.int.esplanator تاريخ زيارة الموقع 12/10/2019

(476) www.mof.gov.jo. تاريخ زيارة الموقع 13/10/2019

(477) يراجع في هذا الإطار، المواد 22، 23، 24، 30، 31، 33 من الاتفاقية العربية لمكافحة الجرائم المعلوماتية.

– اتفاقية بين لبنان واليونان بشأن المساعدة المتبادلة في القضايا المدنية والتجارية والجزائية وتنفيذ الأحكام والقرارات التحكيمية والاسترداد الموقعة في بيروت بتاريخ 5/4/1975.

– اتفاقية التعاون القضائي بين لبنان وإيطاليا المبرمة بتاريخ 10/7/1970.

– الاتفاقية بين لبنان والأردن لسنة 1954.

– اتفاقية تعاون قضائي بين لبنان وسوريا عام 1951.

– اتفاقية تسليم المجرمين بين لبنان واليمن لعام 1949. رغم ذلك، فإننا في حالة نقص في التشريع الدولي في ظل عدم وجود اتفاقية حول الجرائم المعلوماتية بجميع أشكالها ومنها جريمة الاحتيال الإلكتروني سيما وأن هذا النوع من الجرائم يمتاز بالخطورة كونه عابرا للحدود ويسهل ارتكابه ويصعب إثباته[478].

**الخاتمة**

في ختام البحث في موضوع جريمة الاحتيال الإلكتروني، نأمل ان نكون قد حققنا الهدف المتمثل بالقاء الضوء على هذا الموضوع وذلك للأهمية الكبيرة التي يتمتع بها في عصرنا الحالي إذ إن مكافحة هذه الجريمة ينتج عنها حماية مصالح مستخدمي الوسائل الإلكترونية وشبكة الإنترنت.

هذا وسوف نختم بحثنا هذا ببيان أهم النتائج التي تم التوصل إليها والتوصيات التي نقترحها.

تناولنا في هذا البحث جريمة الاحتيال الإلكتروني من حيث ماهيتها والأساليب الحديثة التي يلجأ اليها المحتال لاستخدامها كمناورات احتيالية بهدف إيقاع أكبر عدد من الضحايا وحملهم على تسليم المال. وأوضحنا أن البرامج تدخل من ضمن الاشياء التي تصلح أن تكون موضوعا لجرم الاحتيال الإلكتروني وسندا لقيمتها الاقتصادية. كما أظهرنا الفرق بين الاحتيال العادي والإلكتروني لجهة المناورات الاحتيالية ولجهة تسليم المال.

هذا وقد تبين لنا انه لا يمكن الإدلاء بوجود جرم احتيال إلكتروني عن غير قصد.

ونظرا لحداثة الجرائم الإلكترونية وخاصة جريمة الاحتيال الإلكتروني، ورغم بحثنا الدقيق لاحظنا ندرة الأحكام القضائية التي تتعلق بهذه الجريمة. وبما أن جريمة الاحتيال الاكتروني من جرائم التقنية الحديثة، فإن الكشف عنها يتطلب خبرة فنية متخصصة. **هذا فيما يتعلق بالنتائج.**

**أما فيما يتعلق بالتوصيات،** فإننا نوصي بضرورة تنفيذ قانون المعاملات الإلكترونية والبيانات ذات الطابع الشخصي، والصادرة بتاريخ 2018-10-10 كخطوة أولى مع إعادة النظر بالثغرات المتواجدة فيه فضلا عن وجوب تحديث التشريعات الحالية بصورة تتلاءم مع التطور المعلوماتي والتكنولوجي. كما أننا نطالب بتوقيع المعاهدات الدولية الملائمة بغية تأمين التعاون الدولي لمكافحة جريمة الاحتيال الإلكتروني باعتبارها جرائم عابرة الحدود. كذلك لا بد من تدريب أفراد الجسم القضائي على التقنيات الحديثة للعمل على استقصاء وإثبات الجرائم الإلكترونية.

هذا نوصي بضرورة استخدام أحدث انظمة الحماية على جميع المعاملات المالية عبر الإنترنت، فضلا عن ضرورة العمل على توعية مستخدمي الوسائل الإلكترونية والشبكة العنكبوتية بصور الاحتيال الإلكتروني المختلفة.

(478) لورانس الحوامدة، الجرائم المعلوماتية أركانها وآلية مكافحتها، بحث منشور في كلية الحقوق، جامعة طيبة، المملكة العربية السعودية 2016-2017.

## المراجع:

**أولا: المراجع باللغة العربية**

**أ-الكتب:**


- الياس ناصيف،العقود الدولية،العقد الإلكتروني في القانون المقارن،منشورات الحلبي الحقوقية،بيروت 2009
- سمير عاليه،شرح قانون العقوبات(القسم العام)،المؤسسة الجامعية للدراسات والنشر والتوزيع،مجد،بيروت،2002.
- طوني ميشال عيسى،التنظيم القانوني لشبكة الإنترنت،الطبعة الأولى،المنشورات الحقوقية،صادر ،بيروت 2001.
- عاطف النقيب،أصول محاكمات جزائية،دراسة مقارنة,المنشورات الحقوقية,صادر ،بيروت،1993.
- عبد الفتاح سليمان،الاحتيال في العمل المصرفي في الدول العربية وطرق مكافحتها،منشأة المعارف،الاسكندرية،2012.
- عفيفي كامل عفيفي،جرائم الكومبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون،منشورات الحلبي الحقوقية، بيروت،2003.
- علي عبد القادر القهوجي:شرح قانون العقوبات العام،منشورات الحلبي الحقوقية،بيروت،2008.
- محمود نجيب حسني،جرائم الاعتدء على الأموال في قانون العقوبات اللبناني،دراسة مقارنة،دار النهضة العربية، بيروت،1984.
- نائلة قورة،جرائم الحاسوب الآلي الاقتصادية،الطبعة الأولى،منشورات الحلبي الحقوقية،بيروت،2005.
- هدى حامد قشقوشي،جرائم الحاسب الإلكتروني في التشريع المقارن،دار النهضة العربية،القاهرة، دون سنة النشر.
- وسيم الحجار ،الإثبات الإلكتروني،المنشورات الحقوقية،صادر ،بيروت،2002.


**ب-الأبحاث والمقالات**


- ايناس شري،الاحتيال عبر الإنترنت،

www.alarab.com.qa.details.php?docld=92456&issueno=593&secld=15

- لورانس الحوامدة،الجرائم المعلوماتية أركانها وآلية مكافحتها، بحث منشور في كلية الحقوق،جامعة طيبة،المملكة العربية السعودية،2017-2016


**ج-الدوريات والمجلات والمجموعات**


- صادر في التمييز ،القرارت الجزائية،المنشورات الحقوقية،صادر ،بيروت.
- عفيف شمس الدين:المصنف السنوي في القضايا الجزائية،دون دار نشر ،بيروت.
- كساندر ،موسوعة الشأن العام اللبناني،نشرة احصائية توثيقية شهرية،تصدر عن ايدريل ش.م.م،بيروت.
- مجلة العدل،مجلة حقوقية تصدر عن نقابة المحامين في بيروت.


**د-المراجع التشريعية**


- قانون أصول المحاكمات الجزائية اللبناني.
- قانون التجارة البرية اللبنانية.
- قانون العقوبات اللبناني.
- قانون المعاملات الإلكترونية والبيانات ذات الطابع الشخصي.

**ثانيا:المراجع باللغة الفرنسية**

**A-ouvrages:**

-Bouloc Bernard,droit penal general,dalloz,paris,2013.

-Catala Pierre,informatique et droit pebal,travaux de l'institut de sciences criminelles,ed Cujas,1983

-El Chaer Nidal,la criminalite informatique devant la justice penale,Sader,Beirut,2004.

**B-Codes:**

Code penale.

**C-Sites correspondantes:**

-www.aitnews.com

-www.albankdawli.org

-www.begium.be

-www.fbi.gov

-www.interpol.int

-www.legifrance.gouv.fr

-www.mof.gov.jo