

الجوانب الموضوعية لجرائم تقنية المعلومات

الدكتور
محمد خالد ممدوح

2024

دار الفكر الجامعي
30 شارع سوتير - الإسكندرية
ت : 4843132

مقدمة

التطور التكنولوجي والجريمة المعلوماتية:

مع بداية انتشار شبكة الإنترنت لم يكن هناك قلق تجاه الجرائم التي يمكن أن ترتكب على الشبكة، وذلك نظراً لمحدودية استخدامها، حيث كانت قاصرة على أغراض البحث العلمي فقط، علاوة على كونها مقصورة على فئة معينة من المستخدمين وهم الباحثين والعلماء وطلبة الجامعات، كما كانت شبكة الإنترنت تقيم أنشطتها المعلوماتية والثقافية داخل دائرة حدود الفضاء الافتراضي Cyberspace، بوصفه الوسط الملائم لنقل المفردة المعلوماتية بين المواقع الإلكترونية، التي تستقر في الحواسيب الشخصية المنتشرة على رقعة القرية الإلكترونية الكونية الجديدة.

وقد أقامت الشبكة مجدها على ضمان سهولة تدفق المعلومات بين المواقع الإلكترونية، المقيمة على أرض القرية الإلكترونية الكونية، وبين وثائقها، وتوفير انسيابية لمرور البيانات عبر الشبكات الحاسوبية الكوكبية، بما يضمن الاستغلال الأقصى لهذه الموارد، عبر متاهة هائلة من مسالك التشعب، وعلاقات الاندماج، ضمن نسيج رمزي، لا تُعرف له بداية أو نهاية.

لكن مع بزوغ فجر الثورة المعلوماتية La revolution informatique، وتوسع استخدام شبكة الإنترنت وبدء استخدامها في المعاملات التجارية ودخول جميع فئات المجتمع إلى قائمة المستخدمين بدأت تظهر جرائم على الشبكة ازدادت مع الوقت وتعددت صورها وأشكالها، وهذه الجرائم تطلق عليها الدول الجريمة المعلوماتية، أي تلك الجرائم التي تتم عن طريق الكمبيوتر والإنترنت، وهي من أهم وأخطر التحديات التي تواجه المعاملات الإلكترونية.

ويعد الإنترنت ساحة إجرام نموذجية تتحدى الأجهزة الأمنية والقضائية بثغرات قانونية وفراغ تشريعي، فيمكن حالياً القيام بعملية احتيال إلكترونية ترتكب بين أستراليا وأمريكا بينما المنفذون الحقيقيون موجودون في لندن أو جنوب أفريقيا، وهذا الأمر يثير مشاكل قانونية مثل الاختصاص القضائي والاثبات.

ولعل التطور المستمر للإنترنت وتوفير السرية التامة جعلاً من الإنترنت جهازاً مثالياً لتنفيذ العديد من الجرائم بعيداً عن أعين الجهات الأمنية، فقد مكنت شبكة الإنترنت مافيا الجرائم الإلكترونية من نقل المعلومات الخطرة والمحظورة سواء معلومات مخبراتية أو خطط تخريبية أو صور سرية بمجرد الضغط على زر لوحة المفاتيح بدون أدنى مجهود وبدون الخوف من العقاب.

وتعتبر ظاهرة الجرائم المعلوماتية، من المستجدات الإجرامية المستجدة نسبياً، وتستهدف الاعتداء على البيانات والمعلومات والبرامج بكافة أنواعها، فهي جريمة يقترفها مجرمون أذكاء يمتلكون أدوات المعرفة التقنية أو الفنية، وتوجه للنيل من أجهزة الكمبيوتر وشبكات الاتصالات وقواعد البيانات والبرمجيات ونظم التشغيل، مما يظهر مدى خطورة جرائم الكمبيوتر في أنها تمس الحياة الخاصة للأفراد وتهدد الأعمال التجارية بخسائر فادحة، كما قد تنال من الأمن القومي والسيادة الوطنية للدول، وتشيع فقدان الثقة في التعاملات الإلكترونية.

وقد ازدادت مخاطر الجريمة المعلوماتية تفاقماً في ظل بيئة الفضاء الإلكتروني التي تمثلها شبكة الإنترنت، مما أفرز نوعاً جديداً من الجرائم لم يكن معهوداً من قبل ممثلاً في الجرائم عبر الوطنية Transnational Crimes، التي يتخطى مداها حدود الدول بل والقارات، ولم يعد خطرهما أو آثارها محصورة في النطاق الإقليمي لدولة بعينها، الأمر الذي بات يثير بعض التحديات القانونية والعملية أمام الأجهزة المعنية بمكافحة الجريمة.

ونشهد تطوراً ملحوظاً طرأ على أساليب الجرائم المعلوماتية والتي تشمل صناعة ونشر الفيروسات، الاختراقات، تعطيل الأجهزة، انتحال الشخصية، المضايقة والملاحقة، التشهير وتشويه السمعة، صناعة ونشر الإباحية، وجرائم النصب والاحتيال وغيرها من الأفعال الإجرامية، حيث أن هذه الأنماط لم تعد هي الأشكال الوحيدة للجريمة عبر الإنترنت.

ذلك أنه مع تقدم وسائل الاتصالات والمعلومات وذيوع استعمال الكمبيوتر وسهولة استخدام الإنترنت، أدى إلى ظهور نوع جديد من الجرائم أصبحت معه نصوص قانون العقوبات والإجراءات الجنائية التقليدية عاجزة عن مواجهتها أو التصدي لها، ولعل هذا ما دفع غالبية القضاة وجهات التحقيق إلى التعامل مع المجرم المعلوماتي باللجوء إلى تطويع نصوص ومفاهيم القانون الجنائي العادية المتعلقة بالسرقة واتلاف وتدمير الممتلكات والتعدي والأذى الإجرامي.

وقد تباينت الصور الإجرامية لظاهرة الجريمة المعلوماتية وتشعبت أنواعها فلم تعد تهدد العديد من المصالح التقليدية التي تحميها القوانين والتشريعات منذ عصور قديمة، بل أصبحت تهدد العديد من المصالح التي استحدثتها التقنية المعلوماتية بعد اقترانها بالثورة المعلوماتية.

فالمصالح التقليدية التي تحميها كل التشريعات والنظم القانونية منذ زمن بعيد بدأت تتعرض إلى أشكال مستحدثة من الاعتداء بواسطة هذه التقنية الحديثة فبعد أن كان الاعتداء على الأموال يتم بواسطة السرقة التقليدية أو النصب، أصبحت هذه الأموال يعتدي عليها عن طريق اختراق الشبكات المعلوماتية وإجراء التحويلات الالكترونية من أقصى مشارق الأرض الى مغاربها في لحظات معدودة.

أما المصالح المستحدثة، فتتمثل في استحداث مراكز قانونية أفرزتها الحياة الرقمية الجديدة مثل حقوق الملكية الفكرية على تصميم البرامج

المعلوماتية، بالإضافة الى حقوق الملكية الصناعية، والاسم التجاري للمواقع الالكترونية المختلفة، والحقوق الناتجة عن تشغيلها والخدمات التي تقدمها للعملاء.

لقد كان من نتائج التطور التكنولوجي في الوقت الراهن، وجود ثمة علاقة ارتباط قوية بين استخدامات أجهزة الكمبيوتر وارتكاب بعض الجرائم المستحدثة، أي استخدام الكمبيوتر كأداة لارتكاب الأفعال غير المشروعة، وسواء كانت أجهزة الكمبيوتر محلا للجريمة المعلوماتية أو وسيلة لها، فإن الجوهر في الأمر أن تطور الوسائل التكنولوجية نتيجة لثورة المعلومات - والتي تنتشر بسرعة هائلة وتغزو مختلف مجالات الحياة - أصبح يزيد من فرص انتشار هذا النوع من الجرائم المستحدثة.

- موضوع البحث:

وعلى ذلك فإن موضوع الكتاب هو دراسة تحليلية مقارنة لنصوص قانون مكافحة جرائم تقنية المعلومات ولائحته التنفيذية من الناحية الموضوعية، بهدف التعرف على أهم المميزات التي تضمنها هذا القانون، والتوصل الى أوجه النقص والقصور التي شابت نصوصه بالمقارنة بالنصوص والقوانين المقارنة الصادرة في ذات الشأن، وذلك من خلال تناول أهم جرائم التعدي على الأنظمة المعلوماتية والجرائم المرتكبة بواسطتها.

- أهمية البحث:

تبرز أهمية هذا البحث في كونه محاولة من الباحث لتسليط الضوء على ظاهرة الإجرام المعلوماتي باعتبارها ظاهرة مستحدثة لا تزال في حاجة ماسة الى مزيد من البحث والدراسة خاصة مع تزايد انتشار هذه الجرائم بشكل واضح في العديد من المجالات وعلى جميع المستويات والاصعدة.

كما تكمن أهمية هذه الدراسة في أنها تقدم دراسة عامة تحليلية لنصوص قانون مكافحة جرائم تقنية المعلومات المصري رقم 175 لسنة 2018 ولائحته التنفيذية من الناحية الموضوعية.

- إشكالية البحث:

هناك حرب تكنولوجية بين المجرمين وجهات إنفاذ القانون، فالمجرمون يسعون بشكل دائم نحو التغلب على التقدم التكنولوجي في وسائل مكافحة الجريمة المعلوماتية، كما أن تأثير الوسائل التكنولوجية التي تستخدم لحماية بيانات الأشخاص وحسابات البنوك وغيرها لمواجهة المنظمات الإجرامية قد يحد من نشاط تلك المنظمات، إلا أن هذا التأثير يكون لفترة قد تطول أو تقصر، ويتوقف البعد الزمني لفاعليتها على مدى قدرة المنظمات الإجرامية على استخدام الوسائل التكنولوجية المضادة، وإذا كان المجرمون قد استفادوا من التطور التكنولوجي في استحداث أساليب جديدة لارتكاب جرائمهم، فإن الضرورة تقتضى وضع حدود جديدة للجريمة المعلوماتية واستحداث أساليب جديدة لمكافحتها.

وننتج عن ذلك أن أفرزت الجريمة المعلوماتية تحديات واضحة للقوانين التي وضعت لمكافحتها، فقد تغيرت الجريمة من صورتها التقليدية المتمثلة في صورتها المادية إلى أخرى معنوية، ونتج من ذلك مشكلة تفسير النصوص القانونية، وحظر القياس في المواد الجنائية ومبدأ الشرعية الجنائية، وهذه العوامل تؤدي إلى إفلات الكثير من مجرمي المعلوماتية من العقوبات.

وترجع إشكاليات البحث إلى ما يتميز به من صفة تقنية، ومفردات ومصطلحات جديدة كالبرامج والبيانات التي تشكل محلا للاعتداء أو تستخدم كوسيلة للاعتداء، كما أن معظم مستندات موضوع الجريمة الإلكترونية عبارة عن تسجيلات إلكترونية تتم عبر شبكات الاتصال

المعلوماتي، ذات طبيعة خاصة متميزة، وذلك راجع إلى عدة عوامل منها طبيعة المال المعلوماتي وحادثة ظهور الكمبيوتر وتقنية تشغيله.

ولهذا أصبح لا يكفي أن يكون الباحث متخصصاً في القانون، بل يتعين عليه أن يكون ملماً بالجوانب الفنية لتكنولوجيا الكمبيوتر والإنترنت ليتمكن من إيجاد الحلول للتحديات والمشاكل القانونية التي تثيرها شبكة الاتصال والمعلومات وجرائمها الإلكترونية، ذلك لأن الباحث القانوني في الأبحاث المتعلقة بالجرائم المعلوماتية إذا كان يجهل المصطلحات الحديثة المتعلقة بتكنولوجيا المعلومات والاتصالات والشبكات، وما استجد منها من مصطلحات مثل الحوسبة السحابية Cloud computing، والذكاء الاصطناعي artificial intelligence، والسايبورج Cyborg، واستشراق الجريمة المعلوماتية، والفضاء الإلكتروني Cyberspace، وانترنت الأشياء، والبوت نت botnet، والإنترنت المظلم، والكلوجر Keylogger، والنودز Nods، والمنصات الإلكترونية، وسلسلة البلوك تشين Blockchain، فإنه بلا شك لن يستطيع إتمام البحث على الوجه المطلوب.

وهو مما استلزم من الباحث الاطلاع على النواحي التقنية للكمبيوتر والإنترنت، وذلك من أجل الإلمام بالجوانب العملية لطرق ارتكاب الجريمة المعلوماتية ووسائل التصدي لها وصولاً لإعطائها التكيف والوصف القانوني الصحيح.

- منهجية البحث:

اعتمد الباحث في هذه الدراسة على المنهج الاستقرائي التحليلي الوصفي المقارن ببعض النصوص والتشريعات العربية والأجنبية، والذي يقوم على استقراء المعلومات والحقائق وتفسيرها وتحليلها، والبحث عن العلاقة بينها، وتقديرها وتقييمها ومقارنتها، وتأصيل عناصره مع تحليل

النصوص القانونية المرتبطة بذلك، وذلك بطريقة متكاملة ومتناسقة من أجل الإلمام والتوسع في الموضوع.

كما اعتمد البحث على المنهج التحليلي للآراء الفقهية المتبعة في هذا الشأن، وذلك وصولاً إلى التحقق من مدي كفاية هذه النصوص في مكافحة ظاهرة الجريمة المعلوماتية، ولإيضاح المسؤولية الجنائية عن جرائم وسطاء تقديم خدمات الإنترنت، والتعرف على أهم الضوابط وسبل وآليات التعاون الدولي في مجال مكافحة هذه الجرائم.

وفي هذا الإطار قضت الضرورة الاستعانة بالدراسات المقارنة في بعض المواضيع لتوضيح نقاط الاختلاف والتشابه بين التشريع المصري وبعض التشريعات الأخرى، وكذلك الاستعانة بالكثير من التطبيقات والسوابق القضائية المتعلقة بهذه النوعية من الجرائم التي ترتكب في البيئة الإلكترونية.

- خطة البحث:

وفي ضوء ما تقدم نقسم الكتاب إلى مبحث تمهيدي وثلاثة فصول للموضوع ويعقبهم خاتمة وذلك على النحو التالي:

المبحث التمهيدي: نخصه لدراسة التطور التاريخي للجرائم المعلوماتية وأدوات وأساليب ارتكابها.

الفصل الأول: الأحكام العامة للجريمة المعلوماتية.

الفصل الثاني: جرائم الاعتداء على أنظمة المعلومات.

الفصل الثالث: الجرائم المرتكبة بواسطة أنظمة المعلومات.



الفهرس

الصفحة	الموضوع
9	مقدمة البحث
12	موضوع البحث
12	أهمية البحث
13	إشكالية البحث
14	منهجية البحث
15	خطة البحث

مبحث تمهيدي

بيئة الجريمة المعلوماتية

17	
19	المطلب الأول: لمحة تاريخية عن جرائم تقنية المعلومات
34	المطلب الثاني: طرق ارتكاب الجريمة المعلوماتية
36	الفرع الأول: أدوات ارتكاب الجريمة المعلوماتية
36	أولاً: جهاز الكمبيوتر
39	ثانياً: شبكة الإنترنت المظلم
42	ثالثاً: فيروسات المعلومات
44	رابعاً: مواقع التواصل الاجتماعي
45	خامساً: أدوات التكنولوجيا المشروعة
45	(أ): ماهية أدوات التكنولوجيا المشروعة
46	(ب): أنواع أدوات التكنولوجيا المشروعة
51	الفرع الثاني: أساليب ارتكاب الجرائم المعلوماتية
	أولاً: أساليب ارتكاب الجرائم المعلوماتية المتعلقة
51	بالأشخاص والأموال

65	ثانياً: أساليب ارتكاب الجرائم المعلوماتية الواقعة على البيانات
----	---

الفصل الأول

71	الأحكام العامة للجريمة المعلوماتية
75	المبحث الأول: ماهية الجريمة المعلوماتية
77	المطلب الأول: تعريف وخصائص الجريمة المعلوماتية
77	أولاً: تعريف الجريمة المعلوماتية
77	(أ): تعريف الجريمة المعلوماتية في الفقه
82	(ب): تعريف الجريمة المعلوماتية في التشريع
83	ثانياً: خصائص الجريمة المعلوماتية
89	المطلب الثاني: أركان الجريمة المعلوماتية
90	أولاً: الركن المادي في الجريمة المعلوماتية
90	(أ): السلوك المادي في الجريمة المعلوماتية
95	(ب): النتيجة الإجرامية في الجريمة المعلوماتية
96	(ج): علاقة السببية في الجريمة المعلوماتية
97	الركن الثاني: الركن المعنوي في الجريمة المعلوماتية
98	الركن الثالث: ركن الشرعية
	الركن الرابع: (الركن المفترض) وقوع الجريمة المعلوماتية
101	أثناء المعالجة الآلية للبيانات
	المبحث الثاني: نطاق تطبيق قانون مكافحة جرائم تقنية
106	المعلومات

107	المطلب الأول: تطبيق القانون من حيث المكان
	الفرع الأول: المبادئ التي تحدد السريان المكاني للجريمة
108	المعلوماتية
109	أولاً: مبدأ الإقليمية
109	(أ): المفهوم التقليدي لمبدأ الإقليمية
	(ب): المفهوم الموسع لمبدأ الإقليمية في نطاق الجريمة
112	المعلوماتية
	(ج): موقف المشرع المصري والقضاء من تحديد
115	مكان ارتكاب الجريمة المعلوماتية
	1- موقف المشرع المصري من تحديد مكان ارتكاب
115	الجريمة المعلوماتية
	2- السوابق القضائية في القضاء الأجنبي من تحديد
118	مكان ارتكاب الجريمة المعلوماتية
123	ثانياً: مبدأ الشخصية
125	ثالثاً: مبدأ العينية
125	رابعاً: مبدأ العالمية
	الفرع الثاني: أثر التقنيات الحديثة على تحديد مكان ارتكاب
127	الجريمة المعلوماتية
128	أولاً: مفهوم تقنية البلوك تشين
130	ثانياً: طريقة عمل تقنية البلوك تشين
132	ثالثاً: أثر تقنية البلوك تشين على مبدأ الإقليمية
	رابعاً: الحلول المقترحة لتحديد مكان ارتكاب الجريمة
134	المعلوماتية

- 137 **المطلب الثاني:** تطبيق القانون من حيث الزمان
- 137 أولاً: تحديد النطاق الزمني للنص الجنائي
- ثانياً: إشكالية سريان القانون من حيث الزمان في الجرائم
- 139 المعلوماتية
- (أ): حالة انفصال لحظة ارتكاب الفعل الإجرامي عن
- 140 تحقق النتيجة
- 143 (ب): الوضع في قانون العقوبات المصري

الفصل الثاني

- 147 **جرائم الاعتداء على أنظمة المعلومات**
- **المبحث الأول:** جريمة الدخول غير المشروع إلى نظام
- 152 المعالجة الإلكترونية
- 153 **المطلب الأول:** ماهية جريمة الدخول غير المشروع
- أولاً: المقصود بالدخول غير المشروع لنظام المعالجة
- 154 الإلكترونية
- (أ): تعريف مصطلح الدخول
- 155 (ب): المقصود بمصطلح غير مشروع
- ثانياً: مفهوم جريمة الدخول غير المشروع في التشريعات
- 158 الوطنية
- (أ): مفهوم جريمة الدخول غير المشروع في القانون
- 158 المصري
- (ب): مفهوم جريمة الدخول غير المشروع في القانون
- 163 المقارن

166	ثالثاً: تحديد محل جريمة الدخول غير المشروع
	رابعاً: اختلاف فعل الدخول غير المشروع عن غيره من
167	الأفعال المشابهة
	(أ): اختلاف جريمة الدخول غير المشروع عن جريمة
167	التخريب العمدى
	(ب): اختلاف الدخول غير المشروع عن اعتراض
169	الرسائل المرسلة بطريقة الكمبيوتر
	(ج): اختلاف الدخول غير المشروع في نظام المعالجة
170	الإلكترونية عن استعماله
172	المطلب الثاني: طرق ارتكاب جريمة الدخول غير المشروع.
177	المطلب الثالث: أركان جريمة الدخول غير المشروع
178	الفرع الأول: الركن المفترض في جريمة الدخول غير المشروع
178	أولاً: تعريف نظام المعالجة الآلية للبيانات
179	(أ): المقصود بالمعالجة
179	(ب): ماهية المعالجة الإلكترونية للبيانات
179	1- تعريف المعالجة الإلكترونية في القانون المصري
181	2- تعريف المعالجة الإلكترونية في القانون المقارن .
183	3- تعريف المعالجة الإلكترونية في الفقه
184	4- العناصر الأساسية للمعالجة الإلكترونية للبيانات ..
185	5- مراحل المعالجة الإلكترونية للبيانات
	(ج): مكونات نظام المعالجة الآلية للبيانات في القانون
186	المصري

190	 ثانياً: ماهية البيانات الإلكترونية
190	 (أ): العلاقة الترابطية بين البيانات المعلومات
191	 (ب): تعريف البيانات الإلكترونية
192	 1- تعريف البيانات الشخصية
195	 2- تعريف البيانات الحكومية
	الفرع الثاني: الركن المادي لجريمة الدخول غير
195	 المشروع
196	 أولاً: الركن المادي في جريمة الدخول غير المشروع
	 (أ): العنصر الأساسي للركن المادي في جريمة الدخول
196	 غير المشروع
	 (ب): حالات تحقق الركن المادي في جريمة الدخول
198	 غير المشروع
	 ثانياً: مدي اشتراط توافر الوسائل التقنية الأمنية لتحقيق
199	 الركن المادي
204	 ثالثاً: النتائج المحتملة لسلوك الدخول غير المشروع
	الفرع الثالث: الركن المعنوي في جريمة الدخول غير
206	 المشروع
206	 أولاً: مفهوم القصد الجنائي
	 ثانياً: القصد الجنائي العام في جريمة الدخول غير
207	 المشروع
	 ثالثاً: القصد الجنائي الخاص في جريمة الدخول غير
210	 المشروع في القوانين الأجنبية

	(أ): القصد الخاص في جريمة الدخول غير المشروع
211	في القانون المقارن
	(ب): القصد الخاص في جريمة الدخول غير المشروع
214	في القوانين العربية
	المبحث الثاني: جريمة البقاء غير المشروع داخل النظام
217	المعلوماتي
217	أولاً: الأساس القانوني لتجريم فعل البقاء غير المشروع
218	ثانياً: تعريف وأركان فعل البقاء غير المشروع
218	(أ): تعريف فعل البقاء غير المشروع
218	(ب): أركان جريمة البقاء غير المشروع
	ثالثاً: أختلاف جريمة البقاء داخل النظام عن جريمة
220	الدخول غير المشروع
	(أ) : الآراء الفقهية حول التكييف القانوني لجريمتي
220	البقاء والدخول غير المصرح بهما
	(1) : جريمة الدخول جريمة ايجابية وجريمة البقاء
220	تتحقق بسلوك إجرامي سلبي
	(2) : اختلاف التكييف القانوني يترتب عليه اختلاف
221	حساب مدة التقادم
	(ب) : أهمية التمييز بين جريمة البقاء داخل النظام
222	وجريمة الدخول غير المشروع
	(1) : حدود كل من جريمتي الدخول والبقاء غير
222	المصرح بهما

- (2) : مدي شمول جريمة الدخول لجريمة البقاء غير المصرح بها 223
- المبحث الثالث: جريمة تجاوز حدود الحق في الدخول إلي**
- نظام المعالجة الإلكترونية 226
- أولاً: الأساس القانوني لتجريم تجاوز حدود الحق في الدخول. 226
- ثانياً: تعريف وأركان جريمة تجاوز حدود الحق في الدخول . 226
- (أ): تعريف جريمة تجاوز حدود الحق في الدخول 226
- (ب): أركان جريمة تجاوز حدود الحق في الدخول 228
- ثالثاً: طرق تحقق جريمة تجاوز حدود الحق في الدخول 229
- (أ): تحقق الجريمة من حيث الزمان 229
- (ب): تحقق الجريمة من حيث مستوي الدخول 230

الفصل الثالث

- الجرائم المرتكبة بواسطة أنظمة المعلومات**
- 233
- المبحث الأول: جريمة الاعتداء على بطاقات الدفع الإلكتروني.**
- 237
- المطلب الأول: ماهية بطاقات الائتمان وأدوات الدفع**
- 239
- الإلكترونية 239
- الفرع الأول: مفهوم بطاقات الائتمان** 240
- أولاً: تعريف بطاقات الائتمان 240
- ثانياً: تقسيم البطاقات من حيث وظائفها 241
- ثالثاً: طرق ارتكاب جريمة الحصول على أرقام وبيانات
- البطاقات الائتمانية 242

	(أ): نسخ البيانات الملقنة للشريط الممغنط بطريق
243	 المغافلة
244	(ب): القرصنة المصرفية عبر شبكة الانترنت
245	(ج): تخليق أرقام البطاقات الائتمانية
246	الفرع الثاني: أدوات الدفع الإلكترونية
247	أولاً: الأوراق التجارية الإلكترونية
247	ثانياً: النقود الإلكترونية
248	ثالثاً: الشيك الإلكتروني
	المطلب الثاني: أركان جريمة الاعتداء على بطاقات الدفع
249	الإلكتروني
250	أولاً: الركن المادي
252	ثانياً: الركن المعنوي
253	ثالثاً: عقوبة جريمة الاعتداء على بطاقات الدفع الإلكتروني
	المبحث الثاني: جرائم اصطناع البريد والمواقع والحسابات
255	الإلكترونية الزائفة
	المطلب الأول: مفهوم جريمة اصطناع البريد الإلكتروني
256	ومواقع الويب والحساب الخاص
256	الفرع الأول: جريمة اصطناع البريد الإلكتروني
257	أولاً: تعريف البريد الإلكتروني
259	ثانياً: طريقة عمل البريد الإلكتروني
	ثالثاً: جريمة اصطناع البريد الإلكتروني ونسبه زوراً إلى
260	شخص

- 261 (أ): مفهوم اصطلاح اصطناع البريد الإلكتروني
- (ب): مدي اعتبار اصطناع البريد الإلكتروني جريمة
- 263 تزوير
- 266 (ج): أشكال جريمة اصطناع البريد الإلكتروني
- 267 (د): أسباب ارتكاب جريمة اصطناع البريد الإلكتروني.
- رابعاً: اختلاف جريمة اصطناع البريد الإلكتروني عن
- 268 غيرها من الجرائم ذات الصلة
- خامساً: أدوات تتبع الدليل الجنائي في جريمة اصطناع
- 271 البريد الإلكتروني
- 274 الفرع الثاني: جريمة اصطناع مواقع الإنترنت
- 274 أولاً: ماهية مواقع الإنترنت
- 276 ثانياً: طريقة الوصول إلى المواقع الإلكترونية
- 278 ثالثاً: مفهوم جريمة اصطناع موقع الويب
- رابعاً: الفرق بين اصطناع موقع الويب واصطناع البريد
- 281 الإلكتروني
- خامساً: اختلاف جريمة اصطناع موقع الويب عن غيرها
- 282 من الجرائم ذات الصلة
- 283 الفرع الثالث: جريمة اصطناع الحساب الخاص الإلكتروني
- 283 أولاً: تعريف الحساب الخاص على مواقع الإنترنت
- 285 ثانياً: مفهوم جريمة اصطناع حساب خاص
- ثالثاً: طريقة ارتكاب جريمة اصطناع الحساب الخاص
- 286 على مواقع الإنترنت

	رابعاً: اختلاف جريمة اصطناع الحساب الخاص عن
288	غيرها من الجرائم ذات الصلة
	المطلب الثاني: أركان جرائم اصطناع البريد والمواقع
290	والحسابات الإلكترونية الزائفة
291	أولاً: الركن المادي
293	ثانياً: الركن المعنوي
	ثالثاً: العقوبة المقررة لجريمة اصطناع البريد والمواقع
294	والحسابات الإلكترونية الزائفة
297	الخاتمة
303	قائمة المراجع
321	الفهرس



