المطلب الأول: بعض صور الجريمة المعلوماتية وخصائص المجرم المعلوماتي: تتعدد صور الجريمة المعلوماتية بتعدد الأفعال المكونة لها لذلك سوف نقتصر على ضرب بعض الأمثلة لها فقط الفقرة الأولى :كما تتعدد صفات المجرم المعلوماتي بصفات منفردة عن باقي أصناف المجرمين وخصوصًا من حيث المؤهل العلمي ومن حيث الذكاء ومن حيث الكفاءة في المجال المعلوماتي الفقرة الثانية الفقرة الأولى: بعض صور الجريمة المعلوماتية إذا كانت الجريمة المعلوماتية تتميز بالخصائص التالية: أنها جريمة مستحدثة، ومن الجرائم الناعمة ويصعب إثباتها فإن الجرائم الواقعة على النظام البرمجي أي النظام المعلوماتي المكون من البرامج الحاسوبية التشغيلية والتطبيقية تعتبر من بين صور الجريمة المعلوماتية بالإضافة إلى الصورة المتمثلة في الاعتداء على المعلومات التي يحتويها النظام المعلوماتي يقصد بالبرامج كل ما تم إعداده بواسطة مبرمجين وخبراء متخصصين في التخطيط والبرامج لخدمة أهداف معينة حيث تتحقق هذه الصورة عندما يقوم المجرم المعلوماتي بتعديل البرنامج أو التلاعب فيه أو بزرع برنامج فرعي غير مسموح به في البرنامج الأصلي مما يسمح له بالدخول غير المشروع في العناصر الضرورية لأي نظام حاسوبي وذلك بغية تحقيق ربح مادي كما تتحقق هذه الصورة كذلك عندما يتم تزويد البرنامج الأصلي بمجموعة تعليمات إضافية يسهل الوصول إليها بواسطة شفرة تسمح بالحصول على جميع المعطيات التي يتضمنها النظام الحاسوبي ومثال ذلك توظيف وتصميم برنامج وهمي من خلال قيام المبرمج بوضع برنامج وهمي يصعب اكتشافه يخصص لارتكاب الجريمة ومراقبة تنفيذها. بل ولها تكوين محترف في هذا المجال وربما ذكاء خارق مما يصعب مهمة المحققين في الوصول إلى الحقيقة. فأما صورة استبدال المعلومات فتسمى بجرائم الغش أو التزوير في المعلوماتي كاستبدال رقم بآخر، لأنه حالة نجاحه يستمر فترة طويلة من الزمن أما مسح وحذف المعلومات فيعد من أسهل طرق الإتلاف وذلك كإزالة جزء من المعطيات المسجلة على دعامة الحاسوب والموجودة داخل النظام أو تحطيم تلك الدعامة أو نقل وتخزين جزء من المعطيات إلى المنطقة الخاصة بالذاكرة الفقرة الثانية: صفات المجرم المعلوماتي وأصنافه يتصف المجرم المعلوماتي بمجموعة من الصفات، التي تجعله متميزا عن باقي أصناف المجرمين وسوف نلخص هذه الصفات فيما يلي: حيث غالبًا ما يبحث هذا الصنف من المجرمين عن تكوين أنفسهم في مجال المعلومات بشكل ماهر وخصوصًا تكوين أنفسهم في مجال تقنيات إنشاء التطبيقات الإلكترونية وكذا كيفية استعمالها. ـ الاعتياد المجرم المعلوماتي، من المجرمين الذين يعتادون الإجرام بصفة مستمرة ولذلك نجد في معظم القضايا الجنائية أن هذا الصنف من المجرمين يكون قد اعتاد ارتكاب الجرائم المعلوماتية مما يخلق له نوعًا من الثقة بالنفس في الاستمرار بتلك الخروقات. ـ الاحتراف: المجرم المعلوماتي مجرم محترف لأنه يحترف هذا النوع من الإجرام لأغراض شخصية أو لتحقيق أرباح مادية أو غيرها من المصالح. ـ عدم اتصافه بالعنف: المجرم المعلوماتي لا يتميز بالعنف، وذلك الطبيعة هذا النوع من الجرائم التي ترتكب جلها وهم الذين يقومون باختراق الحواجز الأمنية الخاصة بأنظمة الحواسيب الآلية غير (hackers) عن بعد وبشكل ـ فئة الهاكرز المصرح لهم بالدخول إليها بغية إثبات احترافيتهم في الاختراق، وقد تكون أهدافهم متعددة، وقد كلف التحقيق مبالغ مالية طائلة. حيث يقومون باختراق أنظمة آلات الحاسوب بغية الاطلاع على البيانات المخزنة ، ومن قضايا الاعتداء التي خلفتها الجرائم المعلوماتية في سبتمبر 2016، وفي ديسمبر ومثلهم كمثل المحاسب الذي يقوم بتخريب البرامج المعلوماتية، 3. المطلب الثاني: مكافحة الجريمة المعلوماتية تشريعيًّا 03 المتعلق بالمساس بنظم المعالجة الآلية كما أشرنا إليه سابقًا من القوانين الرادعة لمثل هذا النوع من الإجرام المعلوماتي فما بعض الجرائم المعلوماتية التي نص عليها هذا القانون المغربي ؟ الفقرة الأولى). وما المعاهدات التي صادق عليها المغرب لمكافحة هذا النوع من الجرائم؟ الفقرة الثانية). رقم 20. 05 (القانون رقم 20. ـ القانون المتعلق بالتبادل الإلكتروني للمعطيات القانونية، 05 المتعلق بالتبادل الإلكتروني للمعطيات القانونية الصادر بتاريخ 30 نوفمبر (2007). 08 القاضي بتحديد تدابير لحماية المستهلك، 2011 الصادر بتاريخ 18 فبراير (2011). 09 القانون رقم 08. 09 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع ولذلك سنشير بالدراسة فقط إلى صورتين من صور الجريمة المعلوماتية، كما تم النص عليهما وعلى عقوباتهما في القانون 07. 03 المتعلق بجرائم نظم المعالجة الآلية للمعطيات، هما: ثانيًا: جريمة الاعتداء على منتجات النظام الآلي. 3. 1. 1 جريمة الدخول الاحتيالي إلى نظام المعالجة الآلية للمعطيات نظم المشرع المغربي هذه الجريمة بالمساس بنظم المعالجة الآلية للمعطيات الذي ينص على ما يلي: يعاقب بالحبس من شهر إلى ثلاثة أشهر وبالغرامة من 2000 إلى 10000 درهم أو بإحدى هاتين العقوبتين فقط كل من دخل إلى مجموع أو بعض نظام المعالجة الآلية للمعطيات عن طريق الاحتيال. ويعاقب بنفس العقوبة من بقي في نظام المعالجة الآلية للمعطيات، أو في جزء منه كان قد دخله عن طريق الخطأ وهو غير مخول له حق دخوله. وتضاعف العقوبة إذا نتج عن ذلك حذف أو تغيير المعطيات المدرجة في نظام

المعالجة الآلية للمعطيات، حيث يتمثل الركن المادي لهذه الجريمة في كل من أفعال الدخول إلى مجموع أو بعض نظام المعالجة الآلية للمعطيات عن طريق الاحتيال حيث تعتبر هذه الجريمة من الجرائم الشكلية التي لا يستلزم فيها المشرع من القاضي الجنائي إثبات النتيجة وكذا العلاقة السببية لتحققها. ولذلك يدخل ضمن هذه الأفعال الاحتيالية التي يتحقق بها الركن المادي لهذه الجريمة على سبيل المثال ما يلي: وكذلك الدخول لتطبيق بنكي خاص بالغير. وكذلك الدخول إلى موقع محصن كل من دخل. عن طريق الاحتيال. وهو نفس توجه المشرع الفرنسي الذي يجرم كذلك الدخول غير المصرح به للنظام المعلوماتي كحماية غير مباشرة له ولقد عاقب المشرع الفرنسي على هذه الجريمة بعقوبة حبسية تقدر بسنتين حبسًا وبغرامة مالية تقدر بحوالي 60000 أورو. وينهج المشرع البلجيكي نفس النهج : حيث يعاقب بالحبس من ثلاثة أشهر إلى سنة وبالغرامة، وإذا ارتكبت الجريمة عن طريق الاحتيال تشدد العقوبة وتصبح من ستة أشهر إلى سنتين ولا يقصد من مفهوم الدخول غير المصرح به الدخول المادي بل الدخول المعنوي وتعرف هذه العمليةباسم التداخل أو الالتقاط(Tappolet, p351 .أي الاتصال بالنظام محل الحماية بالطرق الفنية المعلومة المعلوماتي كما عاقب المشرع المغربي بالعقوبة نفسها كل من دخل عن طريق الخطأ وبقي في النظام المعلوماتي أو في جزء منه وهو غير مسموح له بالدخول إليه. وضاعف المشرع المغربي هذه العقوبة في الأحوال التي تتسبب فيها أفعال الدخول أو البقاء في حذف أو تغيير أو تعديل للمعطيات المضمنة بنظام المعالجة الآلية للمعطيات أو أحدثت اضطرابا في سيره واشتغاله. كما شدد المشرع العقوبة في حالة ترتبت نتيجة معينة عن ارتكاب هذه الجريمة المعلوماتية من طرف موظف أو مستخدم في أثناء مزاولة مهامه أو بسببها أو إذا سهل للغير القيام بها سواء أكانت النتيجة هي تغيير المعطيات والبيانات المضمنة بنظم المعالجة الآلية للمعطيات أو القيام بحذفها أو كانت هي إحداث اضطراب في سير واشتغال النظام كل شخص يقوم بالدخول غير المشروع لإلغاء بيانات خاصة، أو حذفها، أو تدميرها، أو إتلافها، أو تغييرها، أو إعادة نشرها. ويقصد بالدخول غير المشروع وفق نظام مكافحة جرائم المعلوماتية السعودي: دخول الشخص بطريقة متعمدة إلى حاسب آلي ، أو موقع إلكتروني أو نظام معلوماتي، ويلاحظ أن المشرع السعودي قد قيد تجريم الدخول غير المصرح به لنظام الكمبيوتر فاشترط بأن يتوافر القصد الخاص لدى المتهم المتمثل في ضرورة تأثير الدخول في نظام الكمبيوتر، ٢- جريمة الاعتداء على منتجات النظام الآلي للمعطيات تجرم القانون الجنائي المغربي كل من أدخل معطيات في نظام المعالجة الآلية للمعطيات أو أتلفها أو حذفها منه أو غير المعطيات المدرجة فيه أو غير طريقة معالجتها، أو طريقة إرسالها عن طريق الاحتيال وذلك كيفما كانت الوسيلة المعتمدة سواء وسائل مادية أو معنوية حيث تكون وسائل الاعتداء مادية إذا وقعت هذه الأفعال على الأجهزة المادية للنظام أو منعت من الوصول إليها. وذلك للخطورة الإجرامية لمثل هذه الأفعال على الغير. ونقصد بالتزوير كل فعل يقوم به الشخص من أجل الدخول إلى نظام المعالجة الآلية للمعطيات، بغرض تغيير أو محو هذه المعطيات، وتبعًا لمقتضيات الفصل 607-6 من مجموعة القانون الجنائي المغربي وكذا الفصل 133 من القانون الجنائي المغربي، فمثلًا جريمة الدخول والبقاء غير المشروع داخل نظام المعالجة الآلية للمعطيات لا تقوم إلا بإثبات عنصر العمد المتمثل في ضرورة إثبات أن الدخول قد تم عن طريق الاحتيال، كما عاقب المشرع كذلك حتى على مجرد محاولة القيام بالجريمة المعلوماتية، إذا تحققت شروط هذه المحاولة. وذلك في دورتها رقم 109، وقد تم إعطاء المجال للانضمام والتوقيع عليها بالمؤتمر الدولي الذي أقيم ببودابست بدولة المجر بتاريخ 23-11-2001، ولقد تم اعتماد هذه الاتفاقية والعولمة convergence لإيجاد الحلول لمجموعة من الإشكالات التي طرحتها الدول لمكافحة ومحاربة هذه الجريمة، والتقارب المستمرة لشبكات الحاسب الآلي والقلق من استخدام هذه الشبكات والمعلومات الإلكترونية لارتكاب جرائم جنائية، واعترافًا منها بالحاجة للتعاون بين الدول والقطاع الخاص في مكافحة جرائم الإنترنت لحماية المصالح المشروعة في استخدام وتطوير تقنيات المعلومات.