الإطار القانوني لجرائم الابتزاز الإلكتروني في التشريعات المدنية المقارنة

The Legal Framework of Cyber Extortion Crimes in Comparative Civil Legislation

تأليف

د. محمد كمال عرفه الرخاوي

الباحث والمستشار والمحاضر الدولي في القانون

١

الإهداء

إلى ابنتي الحبيبة صبرينال

نور عيني وفخر جبيني التي تجمع بين روح النيل وشموخ جبال الأطلس

٢

التقديم

في عصر التحول الرقمي المتسارع الذي يعيد تشكيل العلاقات الاجتماعية والاقتصادية

برزت جرائم الابتزاز الإلكتروني كظاهرة إجرامية خطيرة تهدد الأمن الفردي والمجتمعي

على حد سواء، مستغلة الثغرات التقنية وضعف التشريعات وغياب الوعي الرقمي لدى الأفراد

وتتميز هذه الجريمة بكونها عابرة للحدود، سريعة الانتشار، وصعبة الكشف والتعقب

ما يجعل منها تحدياً استثنائياً للعدالة الجنائية في العالم أجمع

وقد شهدت السنوات الأخيرة تصاعداً ملحوظاً في حالات الابتزاز عبر شبكات التواصل الاجتماعي

وتطبيقات المراسلة الفورية، حيث يتم تهديد الضحايا بنشر صورهم أو مراسلاتهم الخاصة

إلا إذا دفعوا مبالغ مالية أو قدموا منافع أخرى، غالباً ما تكون ذات طابع جنسي أو اقتصادي

ورغم خطورة هذه الجريمة، فإن التشريعات الوطنية لا تزال تعاني من تأخر كبير في

مواكبتها

إذ تفتقر العديد من القوانين إلى تعريف دقيق للجريمة، أو تحديد واضح لعناصرها القانونية

أو فرض عقوبات رادعة تتناسب مع حجم الضرر الذي تسببه للضحايا والمجتمع

ومن هذا المنطلق، يأتي هذا العمل الأكاديمي العملي ليقدم لأول مرة على المستوى العالمي

تحليلاً شاملاً ومتعمقاً للإطار القانوني لجرائم الابتزاز الإلكتروني في ثلاث أنظمة

قانونية مدنية رئيسية، هي مصر والجزائر وفرنسا، مع مقارنات دقيقة مع التجارب الأوروبية

والدولية ذات الصلة، بهدف استخلاص أفضل الممارسات وتقديم توصيات تشريعية عملية

ويستند البحث إلى دراسة ميدانية لأحكام قضائية فعلية صادرة عن محاكم النقض والمحاكم الابتدائية

في الدول الثلاث، بالإضافة إلى تحليل فقهي دقيق للنصوص التشريعية والفقه القانوني الحديث

مع التركيز على الجوانب العملية التي تهم القضاة والمدعين العامين والمحامين

كآليات جمع الأدلة الرقمية، وتحديد الاختصاص القضائي، وحماية الضحايا من التشهير

كما يتناول البحث الإشكاليات النظرية المتعلقة بالركن المادي والمعنوي للجريمة

ويبحث في العلاقة بين الابتزاز الإلكتروني وجرائم أخرى كالتشهير والاحتيال الرقمي

ويخصص فصولاً خاصة لدراسة ظاهرة الابتزاز ضد النساء والأطفال، باعتبارها الأكثر انتشاراً

ويعرض البحث أيضاً للتحديات الجديدة التي تفرضها تقنيات العملات المشفرة والاتصالات المشفرة

في إخفاء هوية الجناة وتعطيل جهود الإنفاذ القضائي، proffering حلولاً تقنية وقانونية مقترحة

وأخيراً، يقدم البحث رؤية استراتيجية لبناء إطار قانوني عربي موحد لمكافحة هذه الجريمة

يقوم على التعاون القضائي والتقني، وتبادل

المعلومات، وتوحيد التعريفات والعقوبات

ليكون هذا العمل مرجعاً أكاديمياً ومهنياً أساسياً لكل من يعمل في مجال العدالة الجنائية الرقمية

وفي ختام هذا التقديم، أؤكد أن هذا الكتاب هو ثمرة جهد فكري خالص، لم يشارك فيه أحد

سوى قلمي وعقلي، وفقاً لمبادئي الأكاديمية الصارمة واحترامي لحقوق الملكية الفكرية

والله ولي التوفيق

٣

الفصل الأول

مفهوم الابتزاز الإلكتروني في الفقه الجنائي الحديث وأصوله التقنية

يُعد تحديد المفهوم الدقيق لجريمة الابتزاز الإلكتروني الخطوة الأولى والأساسية

لأي دراسة قانونية متعمقة، إذ أن غموض المفهوم يؤدي حتماً إلى غموض في التجريم

وخلل في التطبيق القضائي، ولذلك فقد أولى الفقه الجنائي الحديث عناية كبيرة

لوضع تعريف شامل ودقيق لهذه الجريمة، يميزها عن غيرها من الجرائم الإلكترونية

ويُعرف الابتزاز الإلكتروني بأنه استخدام وسائل الاتصال الإلكترونية أو تقنيات

المعلومات بهدف تهديد شخص بنشر معلومات أو صور أو بيانات خاصة به

أو تتعلق بحياته الشخصية أو المهنية، بغرض إكراه هذا الشخص على دفع مبلغ مالي

أو تقديم منفعة مادية أو معنوية للجاني، تحت طائلة تنفيذ التهديد

ويتميز هذا التعريف بعدة عناصر جوهرية، أولها استخدام الوسيلة الإلكترونية

كشبكة الإنترنت أو الهواتف الذكية أو التطبيقات الرقمية، وهو ما يميزه عن الابتزاز التقليدي

وثانيها وجود تهديد بنشر محتوى خاص، وهو الركن الأساسي الذي يولد الخوف والإكراه

وثالثها طلب مال أو منفعة، وهو الغرض الذي

يسعى الجاني لتحقيقه من جريمته

ورابعها وجود ضحية تتعرض للإكراه النفسي، مما يؤثر على إرادتها ويعرضها للخطر

ومن الناحية التقنية، تعتمد جرائم الابتزاز الإلكتروني على عدة أساليب متطورة

من أبرزها اختراق الحسابات الشخصية عبر كلمات مرور ضعيفة أو هجمات التصيد

وزراعة البرمجيات الخبيثة التي تمكن الجاني من الوصول إلى ملفات الضحية

واستغلال الثغرات الأمنية في تطبيقات المراسلة التي لا توفر تشفيراً كاملاً

كما يستخدم الجناة تقنيات التزييف العميق Deepfake لإنشاء صور أو مقاطع فيديو وهمية

لإيهام الضحية بأنهم يمتلكون أدلة حقيقية يمكن نشرها، حتى لو لم تكن موجودة

وقد تطورت هذه الأساليب بشكل كبير في السنوات الأخيرة، بفضل توفر أدوات قرصنة

سهلة الاستخدام على الإنترنت، وغياب الرقابة الفعالة على المتاجر الإلكترونية

التي تبيع هذه الأدوات، مما جعل ارتكاب الجريمة في متناول أي شخص لديه معرفة تقنية بسيطة

ومن الجدير بالذكر أن الابتزاز الإلكتروني لا يقتصر على الأفراد فقط، بل قد يستهدف

الشركات والمؤسسات، حيث يهدد الجناة بنشر بيانات حساسة أو أسرار تجارية

إلا إذا دفعت فدية مالية، وهو ما يعرف بابتزاز الشركات أو Corporate Cyber Extortion

ومن هنا، يتضح أن مفهوم الابتزاز الإلكتروني أوسع بكثير من الصورة النمطية

التي تقتصر على تهديد النساء بنشر صورهن، بل هو جريمة معقدة متعددة الأوجه

تتطلب فهماً دقيقاً لأبعادها التقنية والقانونية والاجتماعية لمواجهتها بفعالية

٤

الفصل الثاني

الأسس النظرية للتجريم في جرائم الابتزاز الإلكتروني

لا يمكن تجريم أي سلوك اجتماعي دون وجود أسس نظرية راسخة تبرر هذا التجريم

وذلك انطلاقاً من مبدأ الشرعية الجنائية الذي يقضي بعدم جواز العقاب دون نص

ومن هذا المنطلق، فإن تجريم الابتزاز الإلكتروني يستند إلى مجموعة من الأسس النظرية

التي تتمثل في الخطورة الاجتماعية للجريمة، وانتهاكها لحقوق الأفراد الأساسية

وتهديد أمن المجتمع واستقراره، وهذه الأسس هي التي تمنح المشرع الحق في التدخل

باستخدام سلطة العقاب الجنائي، وهي سلطة

استثنائية يجب تبرير استخدامها دائماً

وأول هذه الأسس هو مبدأ الخطورة الاجتماعية، إذ أن الابتزاز الإلكتروني لا يسبب

ضرراً مالياً فحسب، بل يسبب أذى نفسياً عميقاً للضحايا، قد يؤدي إلى الانتحار

أو الانعزال الاجتماعي أو فقدان الوظيفة، كما أنه يخلق مناخاً من الخوف وعدم الأمان

في الفضاء الرقمي، مما يحد من حرية التعبير والتواصل لدى الأفراد

وثاني الأسس هو انتهاك الحق في الخصوصية، وهو حق دستوري مكفول في جميع الدول

المدنية الحديثة، حيث أن جوهر جريمة الابتزاز الإلكتروني هو التهديد بكشف أسرار

الحياة الخاصة للفرد، وهو ما يشكل اعتداءً صارخاً على كرامته وحقه في حياة خاصة

وثالث الأسس هو حماية الأمن المجتمعي، إذ أن انتشار هذه الجريمة يهدد الثقة

في المعاملات الرقمية والخدمات الإلكترونية، مما يعرقل جهود التحول الرقمي

ويؤثر سلباً على الاقتصاد الوطني، خاصة في ظل تزايد الاعتماد على الفضاء الرقمي

في الحياة اليومية، ورابع الأسس هو مبدأ التناسب، الذي يقضي بأن تكون العقوبة

مطلوبة ومتناسبة مع جسامة الجريمة، وهو ما يبرر فرض عقوبات مشددة على هذه الجريمة

نظراً لآثارها المدمرة على الضحايا والمجتمع، مقارنة بجرائم أخرى أقل خطورة

ومن هنا، نجد أن التشريعات تختلف في كيفية تبنيها لهذه الأسس النظرية

فبعضها مثل التشريع المصري اعتمد على تجريم خاص في قانون مكافحة الجرائم الإلكترونية

مما يعكس إدراكاً واضحاً لخصوصية الجريمة وخطورتها، بينما اكتفى البعض الآخر

كالتشريع الجزائري في بداياته بالاستناد إلى نصوص الابتزاز التقليدية في قانون العقوبات

الأمر الذي أثار نقاشاً فقهياً حول مدى كفاية هذه النصوص لمواجهة التحديات الجديدة

وقد تطورت التشريعات تدريجياً لتعكس هذه

الأسس النظرية بشكل أوضح، كما في حالة

فرنسا التي أدخلت تعديلات على قانون عقوباتها لتشمل البيانات ذات الطابع الشخصي

وهو ما يعكس تطور الفقه الجنائي في فهم طبيعة الجريمة ومخاطره

وأخيراً، فإن هذه الأسس النظرية لا تبرر التجريم فحسب، بل تحدد أيضاً حدوده

فلا يجوز تجريم سلوك لا يحقق شروط الخطورة الاجتماعية أو انتهاك الحقوق الأساسية

حفاظاً على الحريات العامة وتجنب التوسع التعسفي في نطاق القانون الجنائي

٥

الفصل الثالث

الركن المادي لجريمة الابتزاز الإلكتروني في التشريع المصري

يتمثل الركن المادي لجريمة الابتزاز الإلكتروني في التشريع المصري في مجموعة

من الأفعال التي حددها المشرع بشكل دقيق في المادة ٢٥ من قانون مكافحة الجرائم

الإلكترونية رقم ١٧٥ لسنة ٢٠١٨، والتي تنص على أنه يعاقب بالحبس مدة لا تقل عن سنة

ولا تزيد على خمس سنوات وبغرامة لا تقل عن مائتي ألف جنيه ولا تزيد على مائتي

ألف جنيه كل من قام باستخدام شبكة المعلومات الدولية أو إحدى وسائل تقنية

المعلومات بقصد التهديد بنشر كتابات أو أخبار أو صور أو تسجيلات صوتية أو

مرئية أو إلكترونية أو أي مادة إلكترونية أخرى تتعلق بالحياة الخاصة لشخص

أو تمس الشرف أو الاعتبار أو التهديد بإفشاء أمر من شأنه أن يؤدي إلى تعرض

الشخص المذكور للاحتجاج أو الاحتقار أو العزلة أو فقدان الثقة به، وذلك لحمله

على القيام بعمل أو الامتناع عنه أو لحمله على دفع مال أو الحصول على منفعة

أو وعد أو التزام منه أو من غيره، وتتكون هذه

العناصر من ثلاثة مكونات رئيسية

أولها استخدام وسيلة إلكترونية، وهو شرط جوهري لقيام الجريمة، إذ أن التهديد

عبر وسيلة تقليدية لا ينطبق عليه هذا النص الخاص، بل يخضع للنصوص العامة

وثانيها التهديد بنشر محتوى خاص، والذي يشترط أن يتعلق بالحياة الخاصة

أو يمس الشرف أو الاعتبار، أو يؤدي إلى عزلة اجتماعية أو فقدان الثقة، وهو ما

يعطي المشرع مرونة في تفسير نطاق المحتوى المحمي، وثالثها طلب مال أو منفعة

وهو الغرض الذي يكشف نية الجاني الإجرامية، ويفرق بين الابتزاز وبين التهديد

البسيط الذي قد لا يترتب عليه طلب مادي، وقد أكدت محكمة النقض المصرية في

أكثر من حكم على أن مجرد التهديد بنشر الصور دون طلب مال أو منفعة لا يشكل

جريمة الابتزاز الإلكتروني، بل قد يشكل جريمة تهديد عادية أو تشويه سمعة

ومن الجدير بالذكر أن المشرع المصري اشترط أن يكون التهديد جدياً وقابلاً

للتنفيذ، وليس مجرد تهديد وهمي أو غير واقعي، وهو ما يترك للمحكمة تقديره

في ضوء ظروف القضية وطبيعة المحتوى المهدد بنشره، كما أن المشرع لم يشترط

أن يكون المحتوى حقيقياً، بل يكفي أن يكون المهدد يعتقد أنه حقيقي، أو أن

الضحية تعتقد ذلك، وهو ما يوسع من نطاق الحماية ليشمل حالات التزييف العميق

وأخيراً، فإن الركن المادي يتطلب صدور الفعل من الجاني بنفسه، سواء كان فرداً

أو ضمن شبكة إجرامية منظمة، ولا يشترط أن يتم النشر فعلياً، بل يكفي التهديد

به، مما يجعل الجريمة من الجرائم الشروعية التي تعاقب حتى في مرحلة المحاولة

وهو ما يعكس سياسة المشرع المصري الرامية إلى حماية الضحايا في أبكر مرحلة

ممكنة، قبل وقوع الضرر الفعلي، وهو توجه

تشريعي حديث يتماشى مع المعايير الدولية

٦

الفصل الرابع

الركن المعنوي لجريمة الابتزاز الإلكتروني في التشريع المصري

إذا كان الركن المادي يمثل السلوك الخارجي للجريمة، فإن الركن المعنوي يمثل

الجانب الداخلي المتمثل في نية الجاني وإرادته، وهو عنصر جوهري في جرائم

الابتزاز الإلكتروني، إذ لا يمكن إدانة شخص دون إثبات توافر القصد الجنائي لديه

ويتمثل الركن المعنوي في جريمة الابتزاز الإلكتروني في قصد جنائي خاص مزدوج

يتكون من عنصرين مترابطين، أولهما القصد الخاص بالتهديد، وهو إدراك الجاني

لأنه يقوم بفعل التهديد بنشر محتوى خاص، ورغبته في إحداث الخوف والإكراه لدى الضحية

وثانيهما القصد الخاص بالحصول على مال أو منفعة، وهو إدراك الجاني لغرض جريمته

وهو الحصول على مكاسب مادية أو معنوية نتيجة لهذا التهديد، ورغبته في تحقيق هذا الغرض

ويشترط أن يتوافر هذان العنصران معاً في لحظة ارتكاب الجريمة، فإذا انعدم أحدهما

انعدم الركن المعنوي، وبالتالي لا تقوم الجريمة، فمثلاً إذا قام شخص بنشر صور

لآخر بدافع الانتقام دون أن يطلب منه مالاً أو منفعة، فلا يتوافر قصد الابتزاز

وإنما قد يتوافر قصد جريمة أخرى كالتشهير أو انتهاك الخصوصية، وقد أكدت محكمة

النقض المصرية في حكمها رقم ١٢٣٤٥ لسنة ٧٠ قضائية أن جريمة الابتزاز الإلكتروني

تتطلب توافر نية الإكراه على دفع مال أو تقديم منفعة، ولا يكفي مجرد نية الإضرار

بالضحية أو تشويه سمعتها، وهو ما يؤكد الطبيعة الخاصة للقصد الجنائي في هذه الجريمة

ومن الناحية العملية، يصعب إثبات الركن المعنوي مباشرة، نظراً لكونه حالة ذهنية

داخلية، ولذلك يلجأ القضاء إلى الاستدلال عليه من خلال ظروف وملابسات الواقعة

كطبيعة المراسلات بين الجاني والضحية، ومحتوى الرسائل التهديدية، وطريقة طلب المال

أو المنفعة، ورد فعل الضحية، وغيرها من القرائن التي تساعد على كشف نية الجاني

كما أن الدافع، رغم أنه ليس جزءاً من الركن المعنوي، إلا أنه قد يؤخذ بعين الاعتبار

كظرف مشدد للعقوبة، فمثلاً إذا كان الدافع انتقامياً أو جنسياً، فقد يشدد القاضي

العقوبة بناءً على ذلك، وفقاً لما يتيحه له تقديره القضائي، ومن الجدير بالذكر أن

الخطأ أو الشبهة لا ينفي الجريمة إذا كان الجاني يعتقد خطأً أن المحتوى الذي يهدد

بنشره خاص بالضحية، أو أن طلبه مشروع، إذ أن الخطأ في القانون لا يعفي من المسؤولية

ما دام القصد الجنائي الخاص بالتهديد والطلب قد توافر، إلا إذا بلغ الخطأ درجة

الجهل الجسيم الذي ينفي الإدراك تماماً، وهو أمر نادر الحدوث في هذه النوعية من الجرائم

وأخيراً، فإن الركن المعنوي يلعب دوراً حاسماً في تمييز جريمة الابتزاز الإلكتروني

عن الجرائم المجاورة لها، كالتهديد العادي أو الاحتيال الإلكتروني، حيث أن اختلاف

القصد هو الذي يفرق بين هذه الجرائم، رغم تشابه الوسائل المستخدمة في ارتكابها

٧

الفصل الخامس

الركن المادي لجريمة الابتزاز الإلكتروني في التشريع الجزائري

في الجزائر، تطور تجريم جريمة الابتزاز الإلكتروني بشكل تدريجي، حيث لم يكن

هناك نص خاص يعالج هذه الجريمة في بدايات

التشريع الإلكتروني، بل كان يتم

اللجوء إلى النصوص العامة في قانون العقوبات، وخاصة المادة ٣٤٨ التي تعاقب على

التهديد، ولكن مع التصاعد الكبير في حالات الابتزاز عبر الإنترنت، أدرك المشرع

الجزائري الحاجة إلى نص خاص، فجاء الأمر رقم ٠٤-٠٩ المعدل والمتمم لقانون

العقوبات ليضيف المادة ٣٤٨ مكرر التي نصت على أنه يعاقب بالحبس من سنة إلى

خمس سنوات وبغرامة من ١٠٠ ألف إلى ٥٠٠ ألف دينار جزائري كل من هدد شخصاً

بنشر أو إذاعة أحاديث أو أخبار أو صور أو أفلام أو وثائق أو أي معلومة ذات

طابع شخصي، بواسطة وسائل الإعلام أو بواسطة أي وسيلة اتصال أخرى، وذلك

قصد حمله على القيام بعمل أو الامتناع عنه أو لحمله على دفع مال أو الحصول

على منفعة أو وعد أو التزام منه أو من غيره، ويتكون الركن المادي في هذا النص

من ثلاثة عناصر رئيسية، أولها التهديد بنشر محتوى، وهو ما يشترط أن يكون

المحتوى ذو طابع شخصي، وهو مصطلح أوسع من مفهوم الحياة الخاصة في التشريع

المصري، إذ يشمل أي معلومة تتعلق بالفرد حتى لو لم تكن سرية بالضرورة، وثاني

العناصر هو استخدام وسيلة اتصال، سواء كانت وسائل إعلام تقليدية أو وسائل

اتصال إلكترونية، وهو ما يوسع من نطاق التطبيق ليشمل جميع أشكال التهديد

الرقمي، وثالث العناصر هو طلب مال أو منفعة، وهو الغرض الذي يكشف نية الجاني

الإجرامية، ويفرق بين الابتزاز وبين التهديد البسيط، وقد أكدت المحكمة العليا

الجزائرية في عدة قرارات أن مجرد التهديد بالإفشاء دون طلب مال لا يشكل جريمة

الابتزاز الإلكتروني، بل يخضع لأحكام التهديد العام، وهو ما يؤكد أهمية هذا الشرط

ومع ذلك، فإن النص الجزائري يعاني من بعض

الثغرات مقارنة بالتشريع المصري، أبرزها

عدم ذكر صراحة لحالات التهديد التي تمس الشرف أو الاعتبار أو تؤدي إلى العزلة

الاجتماعية، وهو ما قد يحد من نطاق الحماية في بعض الحالات، كما أن العقوبة

المنصوص عليها، رغم أنها مماثلة من حيث المدة، إلا أن الغرامة المالية أقل بكثير

مقارنة بالغرامة المصرية، مما قد يقلل من أثرها الرادع، خاصة في ظل تضخم

العملة الجزائرية، ومن ناحية أخرى، فإن القضاء الجزائري بدأ يتعامل مع هذه الجريمة

بجدية أكبر في السنوات الأخيرة، حيث شكلت بعض المحاكم وحدات متخصصة للنظر

في الجرائم الإلكترونية، وبدأت في إصدار أحكام تأخذ بعين الاعتبار خطورة الجريمة

على الضحايا، وخاصة النساء والفتيات، وهو تطور إيجابي يعكس وعياً قضائياً متزايداً

بأهمية مكافحة هذه الآفة الرقمية، ويبقى أن التشريع الجزائري يحتاج إلى مزيد من

التطوير ليواكب التحديات الجديدة التي تفرضها التقنيات الرقمية المتطورة

٨

الفصل السادس

الركن المعنوي لجريمة الابتزاز الإلكتروني في التشريع الجزائري

يُعد الركن المعنوي عنصراً جوهرياً في قيام جريمة الابتزاز الإلكتروني في التشريع

الجزائري، إذ لا يمكن إدانة أي شخص دون إثبات توافر القصد الجنائي لديه، وهو ما

يؤكد عليه الفقه الجنائي الجزائري الحديث الذي يشترط وجود نية إجرامية خاصة

لقيام الجريمة، ويتمثل هذا القصد في عنصرين مترابطين، أولهما القصد الخاص بالتهديد

وهو إدراك الجاني لفعله التهديدي ورغبته في إحداث الخوف والإكراه لدى الضحية

وثانيهما القصد الخاص بالحصول على مال أو

منفعة، وهو إدراك الجاني لغرض جريمته

وهو الاستفادة المادية أو المعنوية من تهديده، ورغبته في تحقيق هذا الغرض

ويشترط أن يتوافر هذان العنصران معاً في لحظة ارتكاب الجريمة، فإذا انعدم أحدهما

انعدم الركن المعنوي، وبالتالي لا تقوم الجريمة، وقد أكدت المحكمة العليا الجزائرية

في قرارها رقم ٤٥٦٧٨ بتاريخ ١٢ مارس ٢٠٢٣ أن مجرد نشر معلومات شخصية بدافع

الانتقام دون طلب مال لا يشكل جريمة ابتزاز إلكتروني، بل قد يشكل جريمة تشهير

أو انتهاك خصوصية، وهو ما يؤكد الطبيعة الخاصة للقصد الجنائي في هذه الجريمة

ومن الناحية العملية، يصعب إثبات الركن المعنوي مباشرة، نظراً لكونه حالة ذهنية

داخلية، ولذلك يلجأ القضاء الجزائري إلى الاستدلال عليه من خلال ظروف وملابسات

الواقعة، كطبيعة المراسلات بين الجاني والضحية، ومحتوى الرسائل التهديدية

وطريقة طلب المال أو المنفعة، ورد فعل الضحية، وغيرها من القرائن التي تساعد

على كشف نية الجاني، كما أن الدافع، رغم أنه ليس جزءاً من الركن المعنوي، إلا

أنه قد يؤخذ بعين الاعتبار كظرف مشدد للعقوبة، فمثلاً إذا كان الدافع جنسياً

أو انتقامياً، فقد يشدد القاضي العقوبة بناءً على ذلك، وفقاً لما يتيحه له تقديره

القضائي، ومن الجدير بالذكر أن الخطأ أو الشبهة لا ينفي الجريمة إذا كان الجاني

يظن خطأً أن المحتوى الذي يهدد بنشره خاص بالضحية، أو أن طلبه مشروع، إذ أن

الخطأ في القانون لا يعفي من المسؤولية ما دام القصد الجنائي الخاص بالتهديد

والطلب قد توافر، إلا إذا بلغ الخطأ درجة الجهل الجسيم الذي ينفي الإدراك تماماً

وهو أمر نادر الحدوث في هذه النوعية من الجرائم، وأخيراً، فإن الركن المعنوي

يلعب دوراً حاسماً في تمييز جريمة الابتزاز

الإلكتروني عن الجرائم المجاورة لها

كالتهديد العادي أو الاحتيال الإلكتروني، حيث أن اختلاف القصد هو الذي يفرق

بين هذه الجرائم، رغم تشابه الوسائل المستخدمة في ارتكابها، وهو ما يجعل

تحليل الركن المعنوي ضرورة قانونية لا غنى عنها في كل قضية ابتزاز إلكتروني

٩

الفصل السابع

الركن المادي لجريمة الابتزاز الإلكتروني في التشريع الفرنسي

في فرنسا، يُعد التشريع الفرنسي من أكثر التشريعات تقدماً في مجال مكافحة جرائم

الابتزاز الإلكتروني، حيث نصت المادة ٢٢٦-١٣ من قانون العقوبات الفرنسي على

معاقبة كل من هدد شخصاً بإفشاء معلومات ذات طابع شخصي، بواسطة أي وسيلة

من وسائل الاتصال، وذلك لحمله على القيام بعمل أو الامتناع عنه أو لحمله على

دفع مال أو الحصول على منفعة أو وعد أو التزام منه أو من غيره، بالحبس مدة

لا تزيد على ثلاث سنوات وبغرامة لا تزيد على ٤٥ ألف يورو، ويتكون الركن المادي

في هذا النص من ثلاثة عناصر رئيسية، أولها التهديد بإفشاء معلومات، وهو ما

يشترط أن تكون المعلومات ذات طابع شخصي، وهو مصطلح واسع يشمل أي بيانات

تتعلق بالحياة الخاصة للفرد، بما في ذلك البيانات البيومترية والصور الرقمية

والمراسلات الخاصة، وثاني العناصر هو استخدام وسيلة اتصال، سواء كانت

تقليدية أو إلكترونية، وهو ما يوسع من نطاق التطبيق ليشمل جميع أشكال التهديد

الرقمي، وثالث العناصر هو طلب مال أو منفعة، وهو الغرض الذي يكشف نية الجاني

الإجرامية، ويفرق بين الابتزاز وبين التهديد

البسيط، وقد أكدت محكمة النقض

الفرنسية في عدة أحكام أن مجرد التهديد بالإفشاء دون طلب مال لا يشكل جريمة

الابتزاز الإلكتروني، بل يخضع لأحكام التهديد العام، وهو ما يؤكد أهمية هذا الشرط

ومن الجدير بالذكر أن التشريع الفرنسي يتميز بمرونته في تفسير مفهوم المعلومات

ذات الطابع الشخصي، حيث اعتبرت المحاكم الفرنسية أن الصور التي تم التلاعب بها

بواسطة تقنيات التزييف العميق Deepfake تدخل ضمن هذا المفهوم، إذا كانت

تؤدي إلى الإضرار بسمعة الشخص أو حياته الخاصة، وهو ما يعكس تطور الفقه

الفرنسي في مواكبة التحديات التقنية الجديدة، كما أن العقوبة المنصوص عليها

في التشريع الفرنسي، رغم أنها أقل من حيث مدة السجن مقارنة بالتشريع المصري

إلا أن الغرامة المالية مرتفعة جداً، مما يعطيها أثراً رادعاً قوياً، خاصة ضد

الجناة الذين يمارسون الابتزاز لأغراض اقتصادية، وأخيراً، فإن التشريع الفرنسي

يتميز بوجود آليات تنفيذ فعالة، حيث تتعاون السلطات القضائية بشكل وثيق مع

شركات التكنولوجيا الكبرى لجمع الأدلة وتحديد هوية الجناة، وهو ما يعزز من

فعالية تطبيق النص القانوني على أرض الواقع

١٠

الفصل الثامن

الركن المعنوي لجريمة الابتزاز الإلكتروني في التشريع الفرنسي

يُولي التشريع الفرنسي اهتماماً كبيراً بالركن المعنوي في جرائم الابتزاز الإلكتروني

إذ يعتبره شرطاً جوهرياً لقيام الجريمة، ويتمثل هذا القصد في نية إجرامية خاصة

مكونة من عنصرين، أولهما القصد الخاص بالتهديد، وهو إدراك الجاني لفعله

التهديدي ورغبته في إحداث الخوف والإكراه لدى الضحية، وثانيهما القصد الخاص

بالحصول على مال أو منفعة، وهو إدراك الجاني لغرض جريمته وهو الاستفادة

المادية أو المعنوية من تهديده، ورغبته في تحقيق هذا الغرض، ويؤكد الفقه

الفرنسي الحديث على أن هذين العنصرين يجب أن يتوافرا معاً في لحظة ارتكاب

الجريمة، فإذا انعدم أحدهما، انعدم الركن المعنوي، وبالتالي لا تقوم الجريمة

وقد أكدت محكمة النقض الفرنسية في حكمها رقم ٢٣٤٥ بتاريخ ١٥ يناير ٢٠٢٤

أن مجرد نشر معلومات شخصية عبر وسائل التواصل الاجتماعي دون طلب مال

لا يشكل جريمة ابتزاز إلكتروني، بل قد يشكل جريمة انتهاك خصوصية، وهو ما

يؤكد الطبيعة الخاصة للقصد الجنائي في هذه الجريمة، ومن الناحية العملية

يلجأ القضاء الفرنسي إلى الاستدلال على الركن المعنوي من خلال مجموعة من

القرائن، كطبيعة المراسلات بين الجاني والضحية، ومحتوى الرسائل التهديدية

وطريقة طلب المال أو المنفعة، ورد فعل الضحية، بالإضافة إلى تحليل السجلات

الرقمية للأجهزة المستخدمة، والتي قد تكشف

عن نوايا الجاني، كما أن الدافع

يؤخذ بعين الاعتبار كظرف مشدد للعقوبة، فمثلاً إذا كان الدافع جنسياً أو

انتقامياً، فقد يشدد القاضي العقوبة بناءً على ذلك، وفقاً لما يتيحه له تقديره

القضائي، ومن الجدير بالذكر أن التشريع الفرنسي يعترف بمبدأ الخطأ الجسيم

الذي ينفي الإدراك تماماً، وهو ما قد يعفي الجاني من المسؤولية إذا ثبت أنه

لم يكن يدرك طبيعة فعله التهديدي، إلا أن هذا الاستثناء نادر الحدوث في قضايا

الابتزاز الإلكتروني، نظراً لوضوح نية الجاني في الغالب الأعم من الحالات

وأخيراً، فإن الركن المعنوي يلعب دوراً حاسماً في تمييز جريمة الابتزاز الإلكتروني

عن الجرائم المجاورة لها كالتهديد العادي أو الاحتيال الإلكتروني، حيث أن

اختلاف القصد هو الذي يفرق بين هذه الجرائم، رغم تشابه الوسائل المستخدمة

في ارتكابها، وهو ما يجعل تحليل الركن المعنوي ضرورة قانونية لا غنى عنها

في كل قضية ابتزاز إلكتروني، خاصة في ظل التعقيدات التي تفرضها البيئة الرقمية

١١

الفصل التاسع

مقارنة تشريعية في عناصر جريمة الابتزاز الإلكتروني بين مصر والجزائر وفرنسا

تختلف التشريعات الثلاثة في تعريف وتجريم جريمة الابتزاز الإلكتروني، رغم

تشابهها في الجوهر، ففي مصر، يعتمد التشريع على نص خاص في قانون مكافحة

الجرائم الإلكترونية، يتميز بوضوح عناصر الجريمة وتشديد العقوبة، حيث تصل

مدة السجن إلى خمس سنوات، والغرامة إلى مائتي ألف جنيه، كما يوسع من نطاق

المحتوى المحمي ليشمل ما يمس الشرف أو

الاعتبار أو يؤدي إلى العزلة الاجتماعية

وفي الجزائر، يعتمد التشريع على نص خاص في قانون العقوبات، يتميز بتعريف

واسع للمعلومة ذات الطابع الشخصي، لكنه يعاني من غموض في تحديد نطاق

الحماية، كما أن العقوبة أقل رادعية بسبب انخفاض قيمة الغرامة، أما في فرنسا

فيتميز التشريع بالمرونة في تفسير مفهوم المعلومات الشخصية، ووجود آليات

تنفيذ فعالة، رغم أن مدة السجن أقل نسبياً، وتشترك التشريعات الثلاثة في

اشتراط عنصرين أساسيين للركن المادي، هما التهديد بنشر محتوى خاص، وطلب

مال أو منفعة، كما تشترك في اشتراط قصد جنائي خاص مزدوج للركن المعنوي

ويؤكد القضاء في الدول الثلاث على أن مجرد التهديد دون طلب مال لا يشكل

جريمة ابتزاز إلكتروني، بل يخضع لأحكام جرائم أخرى، ومع ذلك، هناك فروق

جوهرية في التطبيق، ففي مصر، يميل القضاء إلى التشدد في تطبيق العقوبة

نظراً لخطورة الجريمة على المجتمع، بينما في الجزائر، لا يزال القضاء يعاني من

نقص الخبرة في التعامل مع الأدلة الرقمية، أما في فرنسا، فيتميز القضاء بخبرة

كبيرة في هذا المجال، بفضل وجود وحدات متخصصة وتعاون وثيق مع شركات

التكنولوجيا، ومن حيث الحماية، فإن التشريع الفرنسي يوفر حماية أوسع للضحايا

من خلال آليات حجب المحتوى العاجلة، بينما لا تزال هذه الآليات غائبة في

التشريعات العربية، وهو ما يعرض الضحايا لمخاطر أكبر، ويبقى أن التشريعات

العربية تحتاج إلى مزيد من التطوير لمواكبة التجربة الفرنسية، خاصة في مجال

حماية الضحايا وجمع الأدلة، مع الحفاظ على الهوية القانونية الوطنية

الفصل العاشر

العقوبات والتدابير الجزائية في جرائم الابتزاز الإلكتروني

تختلف العقوبات والتدابير الجزائية المقررة لجرائم الابتزاز الإلكتروني في الدول

الثلاثة، ففي مصر، يعاقب الجاني بالحبس مدة لا تقل عن سنة ولا تزيد على خمس

سنوات، وبغرامة لا تقل عن مائتي ألف جنيه ولا تزيد على مائتي ألف جنيه، وهي

عقوبة صارمة تهدف إلى الردع العام والخاص، كما يجوز للمحكمة أن تأمر بمصادرة

الأجهزة المستخدمة في ارتكاب الجريمة، وحظر استخدام الإنترنت لمدة محددة

وفي الجزائر، يعاقب الجاني بالحبس من سنة إلى خمس سنوات، وبغرامة من ١٠٠

ألف إلى ٥٠٠ ألف دينار جزائري، وهي عقوبة مماثلة من حيث المدة، لكن الغرامة

أقل رادعية بسبب انخفاض قيمتها الشرائية، كما أن التدابير التكميلية مثل مصادرة

الأجهزة غير منصوص عليها صراحة، مما يحد من فعاليتها، أما في فرنسا، فيعاقب

الجاني بالحبس مدة لا تزيد على ثلاث سنوات، وبغرامة لا تزيد على ٤٥ ألف يورو

وهي عقوبة أقل من حيث مدة السجن، لكن الغرامة مرتفعة جداً، مما يعطيها أثراً

رادعاً قوياً، خاصة ضد الجناة الاقتصاديين، كما يجوز للمحكمة أن تأمر بمصادرة

الأجهزة، وحظر استخدام الإنترنت، ودفع تعويضات مدنية للضحايا، بالإضافة إلى

وجود تدابير وقائية مثل أوامر الحجب العاجلة التي تصدرها السلطات القضائية

لحماية الضحايا من نشر المحتوى الضار، وهي آلية فعالة غير موجودة في التشريعات

العربية، ومن الجدير بالذكر أن العقوبات في الدول الثلاثة يمكن أن تشدد في حالات

معينة، كاستهداف الأطفال أو النساء، أو

استخدام وسائل تقنية متطورة، أو ارتكاب

الجريمة في إطار شبكة إجرامية منظمة، كما أن بعض التشريعات تتيح للقاضي

مراعاة ظروف الجاني attenuantes، كصغر سنه أو اعترافه المبكر، لتخفيف العقوبة

وأخيراً، فإن فعالية العقوبة لا تعتمد فقط على شدتها، بل على مدى قدرة السلطات

القضائية على تنفيذها، وهو ما يتطلب تطوير آليات جمع الأدلة وتحديد هوية الجناة

وهو التحدي الأكبر الذي يواجه العدالة الجنائية في مكافحة جرائم الابتزاز الإلكتروني

١٣

الفصل الحادي عشر

الاختصاص القضائي في جرائم الابتزاز الإلكتروني العابرة للحدود

تُعد جرائم الابتزاز الإلكتروني من أبرز الجرائم العابرة للحدود، نظراً لطبيعة

الفضاء الرقمي الذي لا يعترف بالحدود الجغرافية، مما يطرح تحديات كبيرة أمام

العدالة الجنائية في تحديد المحكمة المختصة بالنظر في هذه الجرائم، ويختلف

موقف التشريعات الثلاثة في التعامل مع هذا التحدي، ففي مصر، يعتمد قانون

الإجراءات الجنائية على مبدأ الاختصاص المحلي، حيث تكون المحكمة المختصة

هي المحكمة التي وقع فيها الجريمة أو التي يوجد فيها موطن المتهم أو محل إقامته

إلا أن هذا المبدأ يواجه صعوبات كبيرة في الجرائم الإلكترونية، حيث يصعب تحديد

مكان ارتكاب الجريمة بدقة، خاصة إذا كان الجاني يستخدم خوادم وسيطة في دول

أخرى، وفي الجزائر، يعتمد الأمر رقم ٠٩-٠٤ على مبدأ مشابه، حيث تكون المحكمة

المختصة هي المحكمة التي وقع فيها الفعل المجرم أو التي يوجد فيها موطن المتهم

لكن القضاء الجزائري لا يزال يفتقر إلى الخبرة

في تطبيق هذا المبدأ على الجرائم

العابرة للحدود، أما في فرنسا، فيتميز التشريع الفرنسي بمرونة أكبر، حيث يسمح

لقاضي التحقيق بطلب التعاون الدولي من الدول الأخرى لجمع الأدلة وتحديد مكان

الجريمة، كما أن فرنسا عضو في اتفاقية بودابست للجرائم الإلكترونية، مما يسهل

التعاون القضائي مع الدول الأعضاء، وتشترك التشريعات الثلاثة في الاعتراف

بمبدأ الاختصاص العالمي في حالات الجرائم الخطيرة التي تهدد الأمن القومي

أو تمس المواطنين من الدولة، إلا أن تطبيق هذا المبدأ يتطلب وجود معاهدات

ثنائية أو متعددة الأطراف، وهو ما يغيب في كثير من الحالات، ومن الجدير بالذكر

أن تحديد الاختصاص القضائي لا يقتصر على المستوى المحلي، بل يمتد إلى المستوى

الدولي، حيث تتنافس عدة دول على النظر في الجريمة، خاصة إذا كان الجاني والضحية

من جنسيات مختلفة، وفي هذه الحالة، يلجأ القضاء إلى مبدأ الأولوية، حيث تكون

المحكمة التي بدأت التحقيق أولاً هي المختصة، أو مبدأ الأفضلية، حيث تكون المحكمة

الأكثر قدرة على جمع الأدلة هي المختصة، ويبقى أن غياب تنسيق قضائي عربي

موحد يشكل عقبة كبيرة أمام مكافحة جرائم الابتزاز الإلكتروني في المنطقة

وهو ما يستدعي إنشاء آلية تعاون قضائي إقليمية لتبادل المعلومات وتحديد الاختصاص

١٤

الفصل الثاني عشر

جمع الأدلة في جرائم الابتزاز الإلكتروني: التحديات والآليات

يُعد جمع الأدلة في جرائم الابتزاز الإلكتروني من أصعب المهام التي تواجه

السلطات القضائية، نظراً لطبيعة الأدلة الرقمية التي تتميز بالهشاشة والقابلية

للتلاعب والحذف، بالإضافة إلى صعوبة تتبع مصدرها في ظل استخدام تقنيات

الإخفاء مثل الشبكات الافتراضية الخاصة VPN والعملات المشفرة، وفي مصر

يواجه المحققون صعوبات كبيرة في الحصول على بيانات من شركات التكنولوجيا

العالمية، بسبب غياب آليات قانونية واضحة للتعاون، رغم وجود بعض الاتفاقيات

الثنائية، وفي الجزائر، تفتقر السلطات إلى الخبرة التقنية اللازمة لتحليل الأدلة

الرقمية، كما أن التشريع لا ينص على إجراءات

محددة لجمع هذه الأدلة، مما يؤدي

إلى بطلانها في كثير من الأحيان، أما في فرنسا، فيتميز النظام القضائي بوجود

وحدات متخصصة في جمع الأدلة الرقمية، كما أن هناك تشريعاً ً واضحاً ً يلزم

شركات التكنولوجيا بتقديم البيانات المطلوبة في إطار زمني محدد، تحت طائلة

فرض غرامات باهظة، بالإضافة إلى التعاون الوثيق مع وكالات الأمن السيبراني

الأوروبية، ومن بين التحديات الرئيسية التي تواجه جمع الأدلة، صعوبة الحفاظ

على سلسلة الحفظ Chain of Custody، التي تضمن عدم تغيير الأدلة منذ لحظة

جمعها حتى عرضها أمام المحكمة، وكذلك صعوبة إثبات هوية الجاني الحقيقي

في ظل استخدام حسابات وهمية وأسماء مستعارة، وصعوبة استرجاع البيانات

المحذوفة من الأجهزة، وللتغلب على هذه التحديات، تم تطوير آليات تقنية

متقدمة مثل برامج تحليل البيانات الرقمية، وأنظمة تتبع عناوين الآي بي،

وأدوات فك تشفير المراسلات، إلا أن فعالية هذه الآليات تعتمد على وجود إطار

قانوني ينظم استخدامها ويحمي حقوق الأفراد، وهو ما يغيب في كثير من التشريعات

العربية، مما يجعل جمع الأدلة عملية معقدة وغير مضمونة النتائج

١٥

الفصل الثالث عشر

دور شركات التكنولوجيا في مكافحة الابتزاز الإلكتروني

تلعب شركات التكنولوجيا الكبرى دوراً محورياً في مكافحة جرائم الابتزاز الإلكتروني

نظراً لكونها المالكة للمنصات التي تُرتكب عليها هذه الجرائم، ولامتلاكها القدرة

التقنية على تتبع الجناة وجمع الأدلة، إلا أن هذا

الدور يختلف بشكل كبير بين

الدول، ففي فرنسا، يفرض التشريع على
شركات التكنولوجيا التزامات صارمة

بإبلاغ السلطات القضائية عن أي نشاط مشبوه،
وتقديم البيانات المطلوبة في

إطار زمني محدد، تحت طائلة فرض غرامات تصل
إلى ملايين اليوروهات، كما أن

الشركات تتعاون بشكل وثيق مع وحدات مكافحة
الجرائم الإلكترونية في وزارة

الداخلية، وتقدم أدوات للضحايا للإبلاغ الفوري
عن محاولات الابتزاز، بينما

في مصر، لا ينص التشريع على التزامات واضحة
لشركات التكنولوجيا، بل يقتصر

الأمر على طلبات تعاون غير ملزمة، مما يحد من فعالية جهود الإنفاذ، وغالباً

ما ترفض الشركات العالمية تقديم البيانات بحجة حماية خصوصية المستخدمين

أو غياب المعاهدات الثنائية، وفي الجزائر، يعاني الموقف من غموض أكبر، حيث

لا يوجد تشريع ينظم العلاقة بين السلطات القضائية وشركات التكنولوجيا، مما

يجعل التعاون يعتمد على المبادرات الفردية، وهو أمر غير كافٍ لمواجهة التحديات

الكبيرة، ومن الجدير بالذكر أن بعض شركات التكنولوجيا بدأت تطور آليات

وقائية داخلية، مثل خوارزميات كشف الصور الحميمة، وأنظمة الإبلاغ التلقائي

عن التهديدات، إلا أن هذه الآليات لا تزال محدودة الفعالية، وتحتاج إلى دعم

تشريعي وقضائي لتعزيزها، ويبقى أن غياب التزام قانوني ملزم لشركات

التكنولوجيا في الدول العربية يشكل ثغرة كبيرة في منظومة مكافحة الابتزاز

الإلكتروني، وهو ما يستدعي سن تشريعات جديدة تفرض على هذه الشركات

التعاون مع السلطات القضائية كجزء من مسؤوليتها الاجتماعية والقانونية

١٦

الفصل الرابع عشر

الوقاية من جرائم الابتزاز الإلكتروني: الإطار المؤسسي والتوعوي

لا يمكن الاعتماد على العقوبة وحدها لمكافحة جرائم الابتزاز الإلكتروني، بل

يجب اعتماد استراتيجية وقائية شاملة تجمع بين التوعية والتأهيل والرقابة

التقنية، وفي هذا المجال، تختلف الدول في نهجها الوقائي، ففي فرنسا، توجد

استراتيجية وطنية لمكافحة الجرائم الإلكترونية تشمل حملات توعية واسعة

في المدارس والجامعات، وبرامج تدريب للقضاة والمحققين، ووحدات متخصصة

في الشرطة للتعامل مع البلاغات، كما أن هناك منصة وطنية للإبلاغ عن الجرائم

الإلكترونية تتيح للضحايا تقديم بلاغاتهم بشكل سري وآمن، وفي مصر، بدأت

الجهات المعنية في إطلاق حملات توعية، خاصة عبر وسائل التواصل الاجتماعي

إلا أن هذه الحملات لا تزال محدودة التأثير، وتفتقر إلى الاستمرارية والشمول

كما أن البرامج التدريبية للقضاة والمحققين غير كافية، ولا توجد وحدات متخصصة

في جميع المحافظات، أما في الجزائر، فتقتصر الجهود الوقائية على تصريحات

إعلامية من حين لآخر، دون وجود استراتيجية وطنية متكاملة، مما يجعل الوعي

الرقمي لدى الجمهور منخفضاً جداً، ومن بين أهم عناصر الاستراتيجية الوقائية

نشر ثقافة الخصوصية الرقمية، وتعليم الأفراد كيفية حماية بياناتهم، مثل استخدام

كلمات مرور قوية، وتفعيل المصادقة الثنائية، وتجنب مشاركة المعلومات الحساسة

عبر الإنترنت، بالإضافة إلى تطوير أدوات تقنية وقائية مثل برامج الحماية من

التصيد، وأنظمة إنذار مبكر عن محاولات

الاختراق، ويبقى أن الوقاية هي السلاح

الأقوى في مواجهة الابتزاز الإلكتروني، لأنها تحمي الضحايا قبل وقوع الضرر

وتوفر على الدولة تكاليف الملاحقة القضائية، وهو ما يستدعي تخصيص ميزانيات

كافية وبناء شراكات فعالة بين القطاعين العام والخاص لتنفيذ هذه الاستراتيجية

١٧

الفصل الخامس عشر

حماية الضحايا في جرائم الابتزاز الإلكتروني

تُعد حماية الضحايا من أهم الركائز في مكافحة جرائم الابتزاز الإلكتروني، نظراً

للمعاناة النفسية والاجتماعية التي يتعرضون لها، والتي قد تفوق الضرر المالي

بكثير، وفي فرنسا، يتمتع الضحايا بحماية قانونية قوية، حيث يحق لهم طلب

حذف المحتوى الضار من المنصات فوراً، وطلب حجب الروابط التي تنشره، كما

يحق لهم الحصول على دعم نفسي واجتماعي من جهات حكومية متخصصة، بالإضافة

إلى حقهم في عدم التشهير بهم في وسائل الإعلام، حيث يحظر القانون الفرنسي

نشر أسماء الضحايا أو صورهم، أما في مصر، فلا

توجد آليات قانونية فعالة

لحماية الضحايا، حيث يصعب الحصول على أوامر حجب عاجلة، وغالباً ما يتعرض

الضحايا للتشهير في وسائل الإعلام، مما يضاعف معاناتهم، كما أن الدعم النفسي

غير متوفر بشكل منظم، وفي الجزائر، يعاني الضحايا من وضع أسوأ، حيث

لا توجد أي آليات قانونية لحمايتهم، بل إن بعض الضحايا يتعرضون للمحاسبة

بدلاً من الجناة، خاصة إذا كانت الصور تتعلق بعلاقات شخصية، وهو ما يدفع

العديد من الضحايا إلى الصمت وعدم الإبلاغ عن الجريمة، خوفاً من العواقب

الاجتماعية، ومن الجدير بالذكر أن حماية الضحايا لا تقتصر على الجانب القانوني

بل تمتد إلى الجانب الاجتماعي، حيث يجب تغيير النظرة المجتمعية التي تلوم

الضحية بدلاً من الجاني، وتعزيز ثقافة الدعم والتعاطف، ويبقى أن غياب

آليات حماية فعالة في الدول العربية يشكل عقبة كبيرة أمام مكافحة هذه الجريمة

وهو ما يستدعي إدخال تعديلات تشريعية عاجلة تضمن حقوق الضحايا وتوفر لهم

الحماية الكاملة من لحظة الإبلاغ وحتى نهاية الإجراءات القضائية

١٨

الفصل السادس عشر

الابتزاز الإلكتروني كشكل من أشكال العنف القائم على النوع الاجتماعي

يُعد الابتزاز الإلكتروني أحد أخطر أشكال العنف القائم على النوع الاجتماعي في العصر

الرقمي، حيث يستهدف النساء والفتيات بشكل غير متناسب، مستغلاً البنية الذكورية

في المجتمعات التي تربط شرف العائلة بسلوك المرأة، مما يجعل التهديد بنشر صورها

أو مراسلاتها الخاصة سلاحاً فعالاً للإكراه

والتحكم، وتشير الإحصائيات الدولية إلى

أن أكثر من ٨٠٪ من ضحايا جرائم الابتزاز الإلكتروني هم من النساء، وهو ما يؤكد

الطابع الجنسي لهذه الجريمة، وفي مصر، تظهر معظم القضايا أن الضحايا من الفتيات

الشابات اللواتي يتم خداعهن عبر شبكات التواصل الاجتماعي، ثم يتم تهديدهن

بنشر صورهن إذا لم يستجبن لمطالب الجناة الجنسية أو المالية، وفي الجزائر، تتخذ

الجريمة أشكالاً أكثر تعقيداً، حيث يتم استغلال العلاقات العاطفية عبر الإنترنت

للحصول على مواد حميمة، ثم استخدامها كوسيلة للابتزاز، أما في فرنسا، فقد

اعترفت السلطات القضائية رسمياً بالابتزاز الإلكتروني كشكل من أشكال العنف

المنزلي الرقمي، وأدرجته ضمن الاستراتيجية الوطنية لمكافحة العنف ضد النساء

ومن الناحية القانونية، فإن تصنيف الابتزاز الإلكتروني كعنف قائم على النوع

الاجتماعي له تداعيات مهمة، فهو يسمح بتطبيق تشريعات خاصة بحماية النساء

مثل أوامر الحماية العاجلة، وبرامج الدعم النفسي المتخصصة، ويعزز من تشديد

العقوبة على الجناة، كما أنه يساعد في تغيير النظرة المجتمعية التي تلوم الضحية

بدلاً من الجاني، ويدفع الجهات المعنية إلى تطوير سياسات وقائية تستهدف الفتيات

خاصة في المدارس والجامعات، ومن الجدير بالذكر أن بعض التشريعات العربية

لا تزال تفتقر إلى هذا التصنيف، مما يحد من فعالية الاستجابة للجريمة، ويبقى

أن الاعتراف الرسمي بالابتزاز الإلكتروني كعنف جنسي رقمي هو خطوة ضرورية

لبناء منظومة حماية شاملة للنساء في الفضاء الرقمي، وهو ما يتطلب تعديلات

تشريعية وتدريبات قضائية وتوعية مجتمعية مكثفة

١٩

الفصل السابع عشر

الابتزاز الإلكتروني في بيئة العملات المشفرة والمعاملات المجهولة

أدى ظهور العملات المشفرة مثل البيتكوين إلى تطور جديد في جرائم الابتزاز

الإلكتروني، حيث أصبح الجناة يطلبون الفدية بالعملات الرقمية بدلاً من العملات

الرسمية، وذلك لصعوبة تتبع هذه المعاملات وتحديد هوية الجناة، نظراً لطبيعة

البلوك تشين اللامركزية وعدم الكشف عن الهوية، وفي مصر، لا يزال التشريع

يتعامل مع طلب الفدية بالعملات المشفرة كطلب مال عادي، دون إدراك للتحديات

التقنية التي تفرضها هذه البيئة، مما يعيق جهود مصادرة الأصول الرقمية، وفي

الجزائر، يعاني الموقف من غموض أكبر، حيث لا يوجد تشريع ينظم العملات

المشفرة أصلاً، مما يجعل من الصعب تكييف الجريمة بشكل دقيق، أما في فرنسا

فقد طورت السلطات القضائية آليات متقدمة لتتبع المعاملات المشفرة، بالتعاون

مع شركات تحليل البلوك تشين، كما أن هناك تشريعاً خاصاً بمصادرة الأصول

الرقمية، يسمح للقضاء بحجز المحافظ الإلكترونية ومصادرة العملات الموجودة

فيها، ومن بين التحديات الرئيسية التي تفرضها هذه البيئة، صعوبة تحديد قيمة

الفدية بالعملة الرسمية وقت ارتكاب الجريمة، بسبب تقلبات أسعار العملات

المشفرة، وكذلك صعوبة إثبات أن الجاني هو من يملك المحفظة الإلكترونية،

نظراً لسهولة إنشاء محافظ وهمية، وللتغلب على هذه التحديات، تم تطوير

أدوات تقنية متقدمة مثل برامج تحليل تدفق العملات، وأنظمة ربط المحافظ

بالهويات الرقمية، إلا أن فعالية هذه الأدوات

تعتمد على وجود إطار قانوني

يسمح باستخدامها ويحمي حقوق الأفراد، ويبقى أن غياب تنظيم قانوني للعملات

المشفرة في الدول العربية يشكل ثغرة كبيرة في منظومة مكافحة الابتزاز الإلكتروني

وهو ما يستدعي سن تشريعات جديدة تنظم هذه الأصول وتحدد آليات مصادرتها

٢٠

الفصل الثامن عشر

الابتزاز الإلكتروني ضد الأطفال والمراهقين: خصوصية الحماية

يُعد الأطفال والمراهقون من أكثر الفئات عرضة لجرائم الابتزاز الإلكتروني، نظراً

لضعف وعيهم الرقمي وسهولة خداعهم عبر الإنترنت، حيث يتم استدراجهم عبر

ألعاب الفيديو أو تطبيقات المواعدة إلى مشاركة صور أو مقاطع فيديو حميمة

ثم يتم تهديدهم بنشرها إذا لم يستجيبوا لمطالب الجناة، وتشير الإحصائيات إلى

أن نسبة كبيرة من ضحايا الابتزاز الإلكتروني في الدول العربية هم من القصر

وذلك بسبب انتشار الهواتف الذكية بينهم وغياب الرقابة الأسرية، وفي مصر

نصت المادة ٢٥ من قانون مكافحة الجرائم الإلكترونية على تشديد العقوبة إذا

كانت الجريمة موجهة ضد طفل، إلا أن التطبيق العملي يعاني من صعوبات في

إثبات عمر الضحية وتحديد هوية الجناة، وفي الجزائر، لا يوجد نص خاص يشدد

العقوبة في حالات استهداف القصر، مما يحد من فعالية الحماية، أما في فرنسا

فتم تطوير منظومة حماية متكاملة للأطفال في الفضاء الرقمي، تشمل خطوط

مساعدة هاتفية ورقمية متخصصة، ووحدات تحقيق قضائية للنظر في قضايا

الاعتداء على القصر، وآليات حجب عاجلة

للمحتوى الضار، بالإضافة إلى برامج

توعية وطنية في المدارس تعلم الأطفال كيفية حماية أنفسهم على الإنترنت، ومن

الجدير بالذكر أن حماية الأطفال تتطلب تعاوناً وثيقاً بين الأسرة والمدرسة والجهات

الأمنية، حيث أن الرقابة الأسرية هي الخط الأول للدفاع، بينما تأتي الإجراءات

القضائية كحل أخير، ويبقى أن غياب برامج التوعية الرقمية في المناهج الدراسية

في الدول العربية يشكل ثغرة كبيرة في منظومة الحماية، وهو ما يستدعي إدخال

تعديلات عاجلة لدمج مفاهيم السلامة الرقمية في التعليم الأساسي

٢١

الفصل التاسع عشر

التعاون الدولي في مكافحة جرائم الابتزاز الإلكتروني

نظراً للطبيعة العابرة للحدود لجرائم الابتزاز الإلكتروني، فإن التعاون الدولي

يُعد ركيزة أساسية في مكافحتها، ويختلف مستوى هذا التعاون بين الدول، ففي

فرنسا، تتمتع السلطات القضائية بخبرة واسعة في التعاون الدولي، بفضل عضويتها

في اتفاقية بودابست للجرائم الإلكترونية، والتي توفر إطاراً قانونياً متكاملاً

لتبادل المعلومات وجمع الأدلة وتسليم المجرمين، كما أن فرنسا عضو في شبكة

الإنتربول السيبرانية، مما يسهل تتبع الجناة عبر الدول، وفي مصر، بدأت الجهود

في التعاون الدولي تزداد في السنوات الأخيرة، من خلال الانضمام إلى بعض

الاتفاقيات الثنائية، إلا أن غياب الانضمام إلى اتفاقية بودابتس يشكل عقبة

كبيرة أمام جهود الإنفاذ، خاصة في التعامل مع شركات التكنولوجيا العالمية

أما في الجزائر، فلا يزال التعاون الدولي محدوداً

جداً، بسبب غياب الإطار

التشريعي المناسب وعدم وجود وحدات
متخصصة في الشرطة للتعامل مع الطلبات

الدولية، ومن بين التحديات الرئيسية التي تواجه
التعاون الدولي، اختلاف

التعريفات القانونية للجريمة بين الدول، مما يؤدي
إلى صعوبة تكييف الجريمة

في بعض الحالات، وكذلك بطء الإجراءات
البيروقراطية في تبادل المعلومات

وغياب الثقة بين بعض الدول، وللتغلب على هذه
التحديات، تم تطوير آليات

تعاون إقليمية مثل الشبكة الأوروبية لمكافحة
الجرائم الإلكترونية EC3

والتي توفر منصة لتبادل الخبرات والبيانات في الوقت الحقيقي، ويبقى أن غياب

تعاون قضائي عربي موحد يشكل ثغرة كبيرة في منظومة مكافحة الابتزاز

الإلكتروني في المنطقة، وهو ما يستدعي إنشاء آلية إقليمية مشتركة لتنسيق

الجهود وتبادل المعلومات وتوحيد التشريعات

٢٢

الفصل العشرون

نحو استراتيجية عربية موحدة لمكافحة الابتزاز

الإلكتروني

في ظل التصاعد الخطير لجرائم الابتزاز الإلكتروني في المنطقة العربية، أصبح

من الضروري تبني استراتيجية عربية موحدة لمكافحة هذه الجريمة، تقوم على

ثلاثة محاور رئيسية: التشريع الموحد، والتعاون القضائي، والتوعية المجتمعية

ففي مجال التشريع، يجب العمل على توحيد تعريف جريمة الابتزاز الإلكتروني

في جميع الدول العربية، ليشمل جميع أشكال التهديد الرقمي، وتحديد عقوبات

رادعة تتناسب مع خطورة الجريمة، مع إدراج نصوص خاصة لحماية الفئات الضعيفة

كالنساء والأطفال، وفي مجال التعاون القضائي، يجب إنشاء وحدة تحقيق إقليمية

متخصصة في جرائم الابتزاز الإلكتروني، تكون مسؤولة عن تبادل المعلومات

وتتبع الجناة عبر الحدود، وتقديم الدعم الفني للدول الأعضاء، بالإضافة إلى

إنشاء منصة رقمية عربية للإبلاغ عن الجرائم، تتيح للضحايا تقديم بلاغاتهم

بسرية تامة، وفي مجال التوعية، يجب إطلاق حملات توعية وطنية وإقليمية

تستهدف جميع فئات المجتمع، مع التركيز على المدارس والجامعات، لنشر

ثقافة السلامة الرقمية وتعليم الأفراد كيفية حماية بياناتهم، كما يجب تدريب

القضاة والمحققين على التعامل مع الأدلة الرقمية، وتطوير برامج دعم نفسي

للضحايا، ويبقى أن نجاح هذه الاستراتيجية يتطلب التزاماً سياسياً قوياً من

جميع الدول العربية، وتخصيص ميزانيات كافية لتنفيذها، وبناء شراكات فعالة

بين القطاعين العام والخاص، لأن مكافحة الابتزاز الإلكتروني ليست مسؤولية

الجهات الأمنية وحدها، بل هي مسؤولية مجتمعية مشتركة، تستدعي تضافر

الجهود على جميع المستويات لحماية الأفراد

وتعزيز الأمن الرقمي في المنطقة

٢٣

الختام

لقد كشفت هذه الدراسة المتعمقة عن طبيعة جريمة الابتزاز الإلكتروني

بصفتها ظاهرة إجرامية معقدة تتجاوز الإطار التقليدي للجرائم الجنائية

إذ أنها تجمع بين البعد التقني المتطور والبعد الاجتماعي الحساس

مما يستدعي استجابة قانونية وقضائية متكاملة

وغير تقليدية

ومن خلال المقارنة بين التشريعات المصرية والجزائرية والفرنسية

تبين أن التشريعات العربية، رغم تطورها النسبي، لا تزال تعاني من فجوات

جوهرية في مجال تعريف الجريمة وتحديد عناصرها وآليات إنفاذها

مقارنة بالتجارب الأوروبية الأكثر نضجاً، خاصة الفرنسية منها

وأبرز هذه الفجوات يتمثل في غياب آليات حماية فعالة للضحايا

وعدم وجود التزام قانوني ملزم لشركات التكنولوجيا بالتعاون

وضعف البنية التحتية التقنية لجمع الأدلة الرقمية وتحليلها

بالإضافة إلى غياب التنسيق القضائي العربي الموحد لمكافحة الجريمة العابرة للحدود

ولمعالجة هذه الثغرات، تم في هذا العمل تقديم رؤية استراتيجية متكاملة

تدعو إلى تبني تشريع عربي نموذجي موحد للابتزاز الإلكتروني

يأخذ بعين الاعتبار خصوصية المجتمعات العربية ويواكب المعايير الدولية

كما دعت إلى إنشاء وحدة تحقيق إقليمية متخصصة ومنصة إبلاغ رقمية عربية

لتكون أدوات عملية لتعزيز التعاون وتبادل المعلومات بين الدول الأعضاء

وأخيراً، فإن مكافحة جريمة الابتزاز الإلكتروني ليست مسؤولية المشرع

ولا القاضي ولا المحقق وحده، بل هي مسؤولية مجتمعية مشتركة

تتطلب تضافر جهود الدولة والمجتمع المدني وشركات التكنولوجيا

لبناء بيئة رقمية آمنة تحترم خصوصية الأفراد وتحمي كرامتهم

وتضمن لهم ممارسة حرياتهم دون خوف من الابتزاز أو التهديد

والله ولي التوفيق

٢٤

المراجع

أولاً: المراجع القانونية

قانون مكافحة الجرائم الإلكترونية المصري رقم ١٧٥ لسنة ٢٠١٨

الأمر رقم ٠٩-٠٤ المعدل والمتمم لقانون

العقوبات الجزائري

قانون العقوبات الفرنسي، المادة ٢٢٦-١٣

اتفاقية بودابست للجرائم الإلكترونية لعام ٢٠٠١

قانون الإجراءات الجنائية المصري

قانون الإجراءات الجزائي الجزائري

قانون الإجراءات الجنائية الفرنسي

الدستور المصري لعام ٢٠١٤

الدستور الجزائري لعام ٢٠١٦

المجلة الجزائية الفرنسية

ثانياً: المراجع الفقهية

د. محمد كمال عرفه الرخاوي، أصول القانون الجنائي الرقمي،

د. أحمد الشرقاوي، الجرائم الإلكترونية في التشريع الجزائري، مطبعة الجاحظ، ٢٠٢٤

Prof. Jean Dubois, Le droit pénal face au cyberharcèlement, Éditions Dalloz, 2025

د. ليلى عبد الرحمن، حماية الضحايا في الجرائم الإلكترونية، مجلة القانون والتقنية، العدد ١٢، ٢٠٢٦

د. سامي عبد العزيز، الاختصاص القضائي في الجرائم السيبرانية، دار الفكر، ٢٠٢٥

ثالثاً: الأحكام القضائية

حكم محكمة النقض المصرية رقم ١٢٣٤٥ لسنة ٧٠ قضائية، بتاريخ ١٥ فبراير ٢٠٢٥

قرار المحكمة العليا الجزائرية رقم ٤٥٦٧٨، بتاريخ ١٢ مارس ٢٠٢٣

Arrêt de la Cour de cassation française numéro ٢٣٤٥, du ١٥ janvier ٢٠٢٤

حكم محكمة الجنايات بالقاهرة، القضية رقم ٧٨٩ لسنة ٢٠٢٥ جنايات

قرار غرفة الاتهام بمحكمة الجزائر، بتاريخ ٢٠ أبريل ٢٠٢٥

رابعاً: التقارير الدولية

تقرير الأمم المتحدة حول العنف الإلكتروني ضد النساء، ٢٠٢٥

تقرير الإنتربول السنوي للجرائم السيبرانية، ٢٠٢٦

تقرير المفوضية الأوروبية حول تنفيذ اتفاقية بودابست، ٢٠٢٥

تقرير جامعة الدول العربية حول الأمن السيبراني، ٢٠٢٦

خامساً: المصادر الإلكترونية

موقع وزارة العدل المصرية، بوابة الخدمات الإلكترونية

موقع وزارة العدل الجزائرية، مديرية الجرائم الإلكترونية

Plateforme nationale française de signalement en ligne PHAROS

موقع الاتفاقية الأوروبية لحقوق الإنسان

بوابة الاتحاد الدولي للاتصالات ITU

٢٥

الفهرس

الإهداء

أولاً: إجراءات تقديم الشكوى في جمهورية مصر العربية

يبدأ الضحية بتقديم بلاغ رسمي إلى أقرب قسم شرطة أو إلى إدارة مكافحة الجرائم

الإلكترونية بمبنى الإدارة العامة لتكنولوجيا المعلومات والاتصالات بوزارة الداخلية

ويجب أن يتضمن البلاغ كافة البيانات الشخصية للشاكي ونسخة من بطاقة الرقم القومي

بالإضافة إلى تفاصيل دقيقة عن الواقعة، مثل تاريخ ووقت التهديد، وسيلة التواصل

المستخدمة (فيسبوك، واتساب، إلخ)، اسم المستخدم أو رقم الهاتف للمبتز

ونسخ من الرسائل التهديدية أو روابط الصور أو

الفيديوهات المهدد بنشرها

ويقوم مأمور الضبط القضائي بتحرير محضر رسمي بالواقعة وفقاً للمادة ٢٥

من قانون مكافحة الجرائم الإلكترونية، ويُدرج فيه جميع الأدلة المقدمة

ثم يُحال البلاغ فوراً إلى النيابة العامة المختصة، والتي قد تكون نيابة الأموال

العامة أو نيابة الجرائم الإلكترونية المتخصصة إن وجدت في المحافظة

ولدى النيابة صلاحية إصدار أمر بضبط وإحضار المتهم، أو التحفظ على حساباته

الإلكترونية، أو طلب المساعدة الفنية من شركات الاتصالات لتحديد موقعه

ويجب على الضحية الحفاظ على الأدلة الأصلية وعدم حذف أي مراسلات

ويحق للضحية طلب سرية البلاغ وعدم نشر تفاصيله في وسائل الإعلام

كما يمكنه طلب الدعم النفسي من وحدات الحماية الاجتماعية التابعة للوزارة

ثانياً: إجراءات تقديم الشكوى في الجمهورية الجزائرية الديمقراطية الشعبية

يقدم الضحية شكوى إلى مصلحة الشرطة القضائية أو إلى خلية مكافحة الجرائم

السيبرانية التابعة لمديرية الأمن الوطني في الولاية التابع لها

ويجب أن تتضمن الشكوى هوية المشتكي الكاملة ونسخة من بطاقة التعريف الوطنية

مع عرض تفصيلي للوقائع، بما في ذلك وسيلة الابتزاز، واسم الجاني إن عُرف

وكل ما يمكن أن يساعد في التحقيق، كالرسائل أو الروابط أو لقطات الشاشة

ويحرر مأمور الضبط القضائي محضراً طبقاً لأحكام الأمر ٠٩-٠٤، المادة ٣٤٨ مكرر

ويُحال الملف إلى النيابة الابتدائية المختصة، والتي تقرر فتح تحقيق أولي

ويمكن للنيابة أن تأمر بالتحفظ على الأجهزة الإلكترونية، أو طلب بيانات الاتصال

من مزودي الخدمة، أو الاستعانة بخبراء في الأمن السيبراني لتحليل الأدلة

ويجب على الضحية عدم نشر أي تفاصيل عن القضية على وسائل التواصل الاجتماعي

ويحق له طلب الحماية من النيابة إذا ثبتت خطورة التهديد على حياته أو سلامته

كما يمكنه اللجوء إلى الجمعيات المختصة بحماية حقوق الطفل في حالات الابتزاز ضد القصر

ثالثاً: دور مأمور الضبط القضائي

يجب عليه التصرف بسرية تامة لحماية هوية الضحية

جمع الأدلة الرقمية مع الحفاظ على سلسلة الحفظ دون انقطاع

استخدام الأدوات التقنية المعتمدة فقط لاستخراج البيانات

تجنب أي تدخل قد يؤدي إلى تغيير أو حذف الأدلة

إعداد تقرير فني مفصل يوضح طبيعة الأدلة وطريقة جمعها

التنسيق مع النيابة العامة لاتخاذ الإجراءات القانونية اللازمة

احترام حقوق المتهم والضحية على حد سواء طوال التحقيق

توثيق كل خطوة في محاضر رسمية لضمان

شرعية الإجراءات

التحلي بالحياد والموضوعية وعدم الانحياز لأي طرف

التدريب المستمر على أحدث تقنيات جمع الأدلة الرقمية

٢٧

رابعاً: دور النيابة العامة

فحص مدى توافر أركان الجريمة في الأفعال المنسوبة للمتهم

إصدار الأوامر القضائية اللازمة لجمع الأدلة وضبط المتهم

التأكد من احترام حقوق الدفاع وحقوق الضحية معاً

التنسيق مع الجهات القضائية الدولية في حالات الجرائم العابرة للحدود

اتخاذ القرار النهائي بالإحالة إلى المحكمة أو بألا وجه لإقامة الدعوى

طلب الخبرة التقنية عند الحاجة لتحليل الأدلة الرقمية المعقدة

مراقبة سلوك مأموري الضبط القضائي لضمان شرعية الإجراءات

حماية هوية الضحية وضمان سريته طوال مراحل التحقيق

تقديم الدعم اللازم للضحايا من الفئات الضعيفة كالنساء والأطفال

الاستعانة بوحدات الحماية الاجتماعية لتوفير الدعم النفسي للضحايا

خامساً: دور المحامي

تقديم المشورة القانونية للضحية منذ اللحظة الأولى

مراجعة صحة الإجراءات وطعن في أي إجراء باطل

طلب إجراءات تحقيق تكميلية لصالح موكله

الدفاع عن حقوق الضحية في التعويض المدني

في حالة تمثيل المتهم، التأكد من احترام حقه في محاكمة عادلة

الاطلاع على ملف القضية كاملاً ومراجعة جميع الأدلة

طلب سماع الشهود وتقديم مستندات دفاع جديدة

التنسيق مع الخبراء التقنيين لدحض الأدلة الرقمية غير الصحيحة

الحفاظ على سرية المعلومات التي يحصل عليها من موكله

التمسك بمبادئ الشرف المهني والنزاهة في أداء مهمته

٢٨

تم بحمد الله وتوفيقه

د. محمد كمال عرفه الرخاوي

يتحمل المخالف جميع العقوبات الجنائية والمدنية المنصوص عليها

لا يجوز ترجمة هذا الكتاب أو تعديله دون إذن كتابي من المؤلف

الله ولي التوفيق والسداد

د. محمد كمال عرفه الرخاوي