الكلية	القانون
القسم	القانون
المادة باللغة الانجليزية	Cyber Extortion
المادة باللغة العربية	الابتزاز الالكتروني
المرحلة الدراسية	عامة
اسم التدريسي	م.م طه محمود طه ياسين
عنوان المحاضرة باللغة الانجليزية	Electronic blackmail tools
عنوان المحاضرة باللغة العربية	ادوات الابتزاز الالكتروني
رقم المحاضرة	4
المصادر والمراجع	

محتوى المحاضرة

لكل جريمة اداة يقوم المجرم من خلالها بالقيام بفعل او جميع الافعال المكونة لها، و الابتزاز الالكتروني حاله كحال السلوكيات الضارة الاخرى يحتاج الى ادوات وبالأحرى يحتاج الى ادوات خاصة به لا يتم الفعل الا من خلالها، بل ان هذه الادوات هي ما يميز هذا الفعل وتنقل وصفه من الواقعية الى الافتراضية، فمثلاً جريمة القتل تتم بسلاح او قطعة من المعدن او غير ذلك وجريمة السرقة تحتاج الى ادوات متعددة او ربما تنفذ جريمة القتل والسرقة باليد دون الحاجة الى اداة، الا ان الابتزاز الالكتروني يحتاج الى اداة لا يمكن الاستغناء عنها و الادوات المستخدمة في الابتزاز الالكتروني هي معيار وصفه، لذا سنقسم هذا المطلب على فقرتين، نتناول في الاولى الادوات الرئيسية المستخدمة في الابتزاز الالكتروني، ونخصص الفقرة الثانية للأدوات الفرعية المستخدمة في الابتزاز الالكتروني، وكما يأتي:

الفقرة الاولى : الادوات الرئيسية هناك ادوات تتصل اتصالًا مباشرًا بفعل الابتزاز الالكتروني إذ بدونها لا يمكن للمجرم ان ينفذ مخططاته الإجرامية في جريمة الابتزاز الالكتروني ومنها:

١- الحاسب الالي: ويقصد به (كل جهاز إلكتروني يستطع ترجمة أوامر مكتوبة بتسلسل منطقي لتنفيذ عمليات إدخال أو اخراج معلومات إجراء عمليات حسابية أو منطقية، وذلك بأن يقوم الحاسب بالكتابة على أجهزة الاخراج أو التخزين، ويتم ادخال البيانات بواسطة مشغل الحاسب عن طريق وحدة المعالجة المركزية فتتم كتابتها على اجهزة الاخراج)،، وعرفه المشرع المصري بأنه (كل جهاز أو معدة تقنية تكون قادرة على التخزين واداء عمليات منطقية أو حسابية، وتستخدم لتسجيل بيانات أو معلومات أو تخزينها أو تحويلها أو تخليقها أو استرجاعها أو ترتيبها أو تطويرها أو تبادلها أو تحليلها أو للاتصالات)،.

اما المشرع الاردني والمشرع الاماراتي فلم يوردا تعريفا للحاسوب في قوانين الجرائم الالكترونية، وهذا اتجاه محمود لهم لكون جهاز الحاسوب ليس الاداة الوحيدة للجريمة الالكترونية ولاسيما ان المشرع العراقي والمصري لم يوردا تعريفا للأداة الاخرى وهي الهاتف الذكي في قوانينهم بالرغم من حداثة التشريع المصري، لذلك عدم ذكر الاداة يعد الطريق الامثل امام هكذا جريمة متطورة بأدواتها.

ولقد جاء تعريف الحاسوب في مشروع قانون الجرائم المعلوماتية العراقي لسنة ٢٠١١، إذ عرفه في المادة رقم (١) بأنه ((كل جهاز او مجموعة اجهزة مترابطة بعضها مع البعض تقوم بعمليات المعالجة الالية للبيانات)).

اما مشروع قانون مكافحة الجرائم الالكترونية لسنة ٢٠١٩ فقد عرفه بأنه ((اي جهاز الكتروني ثابت او متحرك، سلكي او لاسلكي يحتوي على نظام معالجة البيانات او تخزينها او ارسالها او استقبالها او تصفحها يؤدي وظائف محددة بحسب البرامج والأوامر المعطاة))،.

فهنا نلاحظ ان المشرع العراقي في القانون الجديد اكثر دقة في وضع تعريف الحاسب الالي إذ نلاحظ هنا لمسات خبراء ومختصي المجال المعلوماتي مع المشرع القانوني في وضع هذا التعريف.

ويعد الحاسوب اهم اداة في الجريمة فعن طريقه يقوم المجرم بفعل الابتزاز او اي عمل اخر يمهد للعملية مثل الاستيلاء والحصول على المعلومات او جميع ما سبق من الاعمال.

وقد ذهب رأي من الفقه الى ان الحاسب الالي هو الاداة الوحيدة لارتكاب الجريمة الالكترونية، الا انه وبسبب التطور في المجال التقني، تعددت وسائل التقنية التي تحوي معلومات ويمكن ان تتصل فيما

بينهما، الا اننا لا ننكر دور الحاسب الالي بوصفه اهم ادوات ارتكاب الجريمة وذلك لما يحتويه من برامج تمكنه من الدخول الى شبكات الانترنت، ولانتشاره وسهولة استخدامه،.

واسهم ابتكار الحاسب الالي والشبكة المعلوماتية بشكل كبير في ظهور جرائم لم تكن مألوفة من حيث انواعها واساليبها، فان تطور كلٌّ منهما ادى الى تطور الانماط التي ترتكب فيها الجرائم، كما ادى ذلك الى ظهور جيل جديد من الاجرام، ترتبط جرائمه من حيث الادوات والاساليب بالتطورات التي شهدتها ادوات التقانة الحديثة،.

من خلال ما تقدم يتبين ان دور الحاسب الالي رئيسي وكبير في الجريمة وخاصة في العهد السابق قبل ظهور وسائل تقنية جديدة حجمت من دور الحاسب الالي لكن بشكل نسبي، فلو قمنا ببحث استقصائي على الانترنت لوجدنا انه الاداة الحصرية التي تتم من خلاله الجريمة في الوقت السابق لكن بدأت تدريجيا تأخذ ادوات اخرى حيزاً من الجرمية وهي الهواتف الذكية التي سنبينها لاحقاً.

٢- شبكة المعلومات: عرفت شبكة المعلومات بأسماء عدة على سبيل المثال بـ (شبكة الانترنت) او (الشبكة العنكبوتية) او (الفضاء السبراني) الا ان جميع ما ذكر من تسميات هي تصب في معنى ووصف واحد وتم تسميتها حسب ما اطلقه عليها اغلب المشرعين، وعرفها المشرع المصري بأنها ((مجموعة من الاجهزة او نظم المعلومات تكون مرتبطة معا ويمكن تبادل المعلومات والاتصالات فيما بينها، ومنها الشبكات الخاصة والعامة وشبكات المعلومات الدولية والتطبيقات المستخدمة عليها)) ،، اما المشرع الاردني فقد عرفه بأنها ((ارتباط بين اكثر من نظام معلومات لإتاحة البيانات والمعلومات والحصول عليها))،.

اما المشرع الاماراتي فقد عرفها بأنها ((ارتباط بين مجموعتين أو اكثر من البرامج المعلوماتية ووسائل تقنية المعلومات التي تتيح للمستخدمين الدخول وتبادل المعلومات))،.

وعرفها المشرع العراقي بأنها ((مجموعة من اجهزة الحاسوب أو نظم معالجة المعلومات مترابطة مع بعضها البعض للحصول على البيانات والمعلومات وتبادلها كالشبكات العامة والخاصة والشبكة العالمية لخدمة الانترنت وما في حكمها))،، اما مشروع قانون مكافحة الجرائم الالكترونية العراقي لسنة ٢٠١٩، فقد عرفها في المادة (١) بأنها ((ارتباط بين اكثر من نظام معلوماتي للحصول على المعلومات او تبادلها)).

وعُرفت من الاتفاقية العربية بأنها ((ارتباط بين مجموعتين او اكثر من البرامج المعلوماتية ووسائل تقنية المعلومات التي تتيح للمستخدمين الدخول وتبادل المعلومات))،،

من خلال ما تقدم نرى هناك تقاربًا في التعريفات بين المشرع الاردني والاماراتي والاتفاقية العربية لمكافحة الجرائم المعلوماتية إذ جاء التعريف مقتضباً، الا ان المشرع العراقي عرفها بشكل مفصل وذكر شبكة المعلومات العالمية والمحلية الخاصة ايضا وهذا اتجاه جيد، إذ بالإمكان ان تكون هناك جرائم ابتزاز على نطاق ضيق، إذ تنفذ الجريمة خلال حدود الخادم المحلي داخل نظامه المعلوماتي وحتى يمكن ان يكون الابتزاز داخل المنزل الواحد بين افراد الاسرة من خلال شبكة معلومات خاصة وليست عامة او تنفذ احدى ادوات الجريمة بواسطة الشبكة الخاصة مثل الاستيلاء على المعلومات او سرقتها للقيام بالابتزاز الالكتروني عن طريق شبكة عامة.

وكان لشيوع الشبكة المعلوماتية حول العالم اثر كبير في شتى المجالات ومنه المجال الاجرامي، والخطورة التي تمثلها انها اصبحت وسيلة سهلة للاستخدام السلبي التقني، فضلا عن توسع نطاق اثارها المكاني واللامحدودية التي تشوبها،، وتحتوي ايضا على نظام معالجة الية والذي هو عبارة عن اشارات ونبضات الكترونية تمر خلال نظم معالجة الى شبكات تواصل عالمية ، والذي بالنهاية اصبح يثير تحديات قانونية وعملية امام الجهات المعنية بمكافحة الجريمة،.

٣- الهاتف الذكي : يعرف بأنه (جهاز محمول يعمل وفق نظام تشغيل متطور يمزج بين تقديم خدمات الهواتف التقليدية والحواسب الشخصية بطريقة احترافية تتيح – للمستخدمين عملية تلقي المعلومات والتواصل مع الناس وإنجاز المهمات المختلفة)،، وتتمثل احدى الجوانب السلبية في سوء استخدام الهواتف الذكية هي استخدامها في عملية الابتزاز وقد اسهمت بطريقة او بأخرى في زيادة حالات الابتزاز، من خلال الاستخدام غير المشروع لها، والتقاط الفيديو والصور والتسجيلات الصوتية من خلالها،.

لم يتطرق المشرع العراقي او التشريعات المقارنة الى تعريف للهاتف الذكي الا اننا سنتطرق اليه لكونه اداة اساسية ومهمة للجريمة وربما تنظيم اقتناء مثل هذه الادوات يسهم في تحييد كثير من الافعال الجرمية فأكثر المؤلفات الصادرة قد صدرت واعتمدت على احصاءات غربية في تعداد الوسيلة المستخدمة في الابتزاز الالكتروني و ركنت للحاسوب كأداة اساسية ومن المعلوم ان واقع تلك الدول تختلف اختلافًا جذريًا عن ما نمثله نحن من مجتمعات شرقية وبعلاقة طردية تختلف الجريمة وادواتها

من رقعة جغرافية الى اخرى، فاغلب جرائم الغرب في جريمة الابتزاز ادواتها الحاسب الالي باعتبار ان اكثر جرائم الابتزاز الواقعة في تلك الرقعة الجغرافية تستهدف شركات ومؤسسات بالمعنى (اشخاص معنوية) وعدم اهتمامهم لكثير من اعتبارات العيش التي يهتم بها المواطن الشرقي ومنها اعتبارات الشرف وسمعة الفرد والعائلة، إذ في المجتمعات الشرقية أغلب القضايا هي عبارة عن ابتزاز تخص هذه الاعتبارات واغلب ادواتها هي الهواتف الذكية، ولاسيما بعد ان اصبحت تلك الهواتف بمتناول الجميع، فضلا عن رخص ثمنها نوعاً ما والمواصفات التي تحملها.

ومن مزاياها انها تحتوي على انظمة تشغيل متطورة، ومعالجات وذاكرة مسؤولة عن حفظ البيانات،، والمنافسة بين الشركات المنتجة دفعت بها الى رفع المواصفات لتلك الهواتف من كاميرات وذاكرة حفظ ونظام معالجة، فضلا عن سهولة حفظها واخفائها مما سهل الكثير من الشبان والشابات الى اقتنائها وإخفائها عن ذويهم ووقوعهم في الادمان على تلك الهواتف، ولاسيما بعد ان اصبحت بعض التطبيقات تمنح ارباحاً على نسبة المشاهدة والاشتراك لمتابعي الصفحات الشخصية مما ادى الى ممارسة سلوكيات خاطئة من قبل اصحاب الصفحات لزيادة عدد المتابعين، الذي يقابله غياب الرقابة الحكومية على ما يتم نشره على تلك الصفحات، زد على ذلك الاغلاق التام بسبب جائحة كارونا التي عصفت بالمعمورة واحدها العراق والتي بسببها تم تحويل التعليم الى الكتروني مما دفع العوائل الى السماح لأبنائهم الاحداث باقتناء تلك الهواتف مما زادت سلوكيات الابتزاز بشكل خطير.

ومثال ذلك ما جاء في احد القرارات الصادرة من القضاء العراقي في الابتزاز عن طريق الهواتف ((لدى التدقيق والمداولة وما هو ثابت من سير التحقيق الابتدائي والقضائي والمحاكمة الجارية بحق المدان وقائع الدعوى تتلخص انه بتاريخ ٢٠١٩/٨/٨ وفي منطقة العطيفية نسب الى المتهم (ج) قيامه بنشر صورها الفاضحة التي سبق وان ارسلتها على مواقع التواصل الاجتماعي في حال عدم تسليمها له مبلغًا وقدره من المال حيث سبق وان تعرفت على المتهم على مواقع التواصل وتطورت العلاقة بينهم وقامت بإرسال صورها الشخصية ومن ثم انتهت علاقتهما بعد مدة قام بتهديدها بنشر صورها الموجودة في هاتفه المحمول في حال عدم اعطاء المبلغ المطلوب وتم نصب كمين له من قبل جهاز الامن الوطني، واطلعت المحكمة على محضر ضبط الهاتف وتفريغ الصور، وقد اكتفت المحكمة بالأدلة المقدمة من اعتراف المتهم والمفرزة القابضة ومحضر ضبط الهاتف ومحضر تفريغ الرسائل وان تراجعه عن اعترافه امام المحكمة لم يؤثر على كفاية الادلة وسلامتها فالغاية من هذا الانكار الافلات من العقاب قررت المحكمة ادانة المتهم وفق المادة (١/٤٣٠) من قانون العقوبات))،، وفي قرارات اخرى

في كل من المملكة الاردنية الهاشمية ومصر والامارات العربية المتحدة، إذ في جميع الوقائع التي اطلعت عليها كانت الأدوات المستخدمة في الجريمة هو الهاتف المحمول والتي سنتطرق اليها تباعاً.

الفقرة الثانية: ادوات فرعية

وفي مقابل الادوات الرئيسية في الابتزاز الالكتروني التي بيناها سابقًا، هناك ادوات فرعيه، قد يحتاجها المجرم وقد لا يحتاجها حسب نوع الفعل ودرجة خبرته في المجال المعلوماتي ، لذلك سنبين هذه الادوات على سبيل المثال وليس الحصر بسبب حداثة الابتزاز الالكتروني وسرعة تطوره.

اولا: التطبيقات او البرامج : عرفت بأنها (نوع من البرمجيات المصممة لتعمل على الأجهزة، عن طريق ربطها بخدم الانترنت ويمكن أن تأتي هذه التطبيقات محملة مسبقا على الأجهزة، أو يمكن تحميلها من مخازن التطبيق أو الأنترنت)،، ولم يتطرق المشرع العراقي الى ذكر التطبيق في مشروع قانون مكافحة الجرام المعلوماتية لسنة ٢٠١١، لكنه عرف البرنامج بأنه ((مجموعة من الاوامر التي تجعل النظام قادراً على اداء المعالجة الالية للبيانات))، وايضا لم يتطرق له في مشروع قانون الجرائم الالكترونية لسنة ٢٠١٩ الا انه عرف البرنامج ايضاً،.

وكذلك المشرع المصري فقد عرف البرنامج بأنها ((مجموعة من البيانات والتعليمات والاوامر، القابلة للتنفيذ بوسائل تقنية المعلومات والمعدة لإنجاز مهمة معينة))،.

وقد جاء المشرع الاردني في قانون الجرائم الالكترونية رقم (٢٧) لسنة ٢٠١٥، في المادة (١) في مضمون مقارب لما جاء به المشرعان العراقي والاماراتي، وكانت للاتفاقية العربية لسنة ٢٠١٠ التعريف نفسه في المادة (٢)، اما المشرع المصري فقد جاء بشيء من التفصيل حيث عرفه بأنه ((مجموعة من الاوامر والتعليمات المعبر عنها بأي لغة أو رمز أو اشارة والتي تتخذ أي شكل من الاشكال، ويمكن استخدامها بطريق مباشر او غير مباشر في الحاسب الالي لأداء وظيفة او تحقيق نتيجة، سواء كانت هذه الاوامر والتعليمات في شكلها الاصلي أو في اي شكل اخر تظهر فيه من خلال حاسب الي، او اي نظام معلوماتي((،.

ويمكن ان تكون هذه التطبيقات خاصة بالهاتف الذكي او بالحاسب الالي ومن الممكن ان يتمكن المجرم من القيام بنشاطه عن طريق هذا الجهاز او من خلال التطبيقات فالكثير من الاجهزة عبارة عن قطعة من المعدن ليس لها قيمة بدون هذه التطبيقات .

وعند البحث والاطلاع غالبا ما نجد ان جريمة الابتزاز تتم عن طريق تطبيقات التواصل الاجتماعي مثل الواتساب والفيس بوك والانستغرام وغيرها وهذه التطبيقات يمكن ان يتم تنزيلها مباشرة الى الحاسوب الالي والهاتف، ويمكن فتحها عن طريق متصفح جوجل، اذ تعد هذه التطبيقات احد مصادر التعرض الى الخصوصية، إذ لا ضمان ولا حرمة لأنسان، وعن طريقها يتم نشر الكثير من الامور الخاصة، وبيانات تتعلق بالوضع الصحي والمالي، التي من خلال هذه الامور يختار المجرمون ضحاياهم، وغالبا ما تنتهك هذه التطبيقات الخصوصية عند التسجيل حيث ترغم المستخدم التنازل عن جزء من حقوقه، مما يمكنها من الولوج الى بيانات الهاتف بكل سهولة، وخاصة روابط التي تنتشر بداعي الوظيفة او الجوائز والتي يخسر الكثير من الاشخاص خصوصياتهم بسببها، فضلا عن انها غير حازمة في مسألة التأكد من هوية المشترك فيها، إذ لا يخضع للتدقيق فهذا غير ممكن من قبل ادارة التطبيق لكون بعض التطبيقات يشترك فيها مئات الملايين.

فضلا عن ذلك انها اذا دققت في هويات المشتركين ستفقد الكثير منهم لعدم الرغبة فئات كبيرة تسليم هويتها للأخرين، فضلا عن الروابط التي يتداولها المستخدمون فيما بينهم على اختلاف واجهاتها، فمنها ما تكون على شكل جوائز وهدايا مالية او سيارات، و الاكثر هي روابط لمواقع جنسية او روابط للتقديم على وظائف مستغله حاجة الاشخاص المالية والجنسية وجهلهم بها، مما يؤدي بالنهاية الى اختراق حساباتهم، وبالنهاية يصبح هؤلاء ضحايا لعمليات ابتزاز وغالبا هكذا طرق من عمليات الابتزاز تكون منظمة ومن خارج البلاد مما يصعب ايقافها او الحد منها.

ثانيا: الاجهزة والمعدات الخاصة بفعل الابتزاز الالكتروني: من الممكن ان يحصل المجرم على الاعتبارات المتعلقة بالشخص محل الابتزاز بصورة عرضية، على سبيل المثال عند فقدانها من قبل المجنى عليه في مكان عام (لقطة)،، او اية طريقة اخرى يتمكن منها الجاني الحصول على هذه المعلومات او البيانات او الصور... الخ، او عن طريق الدخول الى حساب المجنى عليه او حاسبه الالي او هاتفه وسرقة تلك البيانات، فبعض المجرمين لديه القدرة على الولوج الى اي جهاز وسرقة بيانات منه.

وهناك من المجرمين لا يمكنهم القيام بذلك الا عن طريق اجهزة اختراق ومعدات خاصة لفك الشفرات والاكواد، او ان الشخص المستهدف يستخدم طرقًا وادوات تمكنه من الحفاظ على ممتلكاته الى الحد الاعلى من الحماية، ويعتقد الباحث ان مقدار البساطة والسهولة في الحصول على تلك المعلومات

تعتمد على درجة خبرة الجاني وحرصه والحيطة والحذر والخبرة لدى المجنى عليه، فكلما كان المجنى عليه على قدر من الالمام بجانب الامن السيبراني واتخاذ تدابير للحماية تكون المهمة على الجاني صعبة اكثر.

وللمعدات والاجهزة الخاصة بالاختراق خطورة كبيرة فالمشرع المصري عاقب عليها بمجرد حيازتها وليس استخدامها،، لذلك تعد من جرام الخطر وليس الضرر، وهذا ما سار عليه المشرع الاماراتي ،، اما المشرع العراقي و الاردني فلم يتطرقا الى الاجهزة والمعدات الخاصة بالاختراق، وايضا الاتفاقية العربية لم تنص على المعدات والاجهزة الخاصة بالاختراق .

رابعا: المعلومة: على الرغم من كونها في بعض الاحيان تعد محلًا للجريمة او ينصب السلوك الاجرامي عليها، الا ان للمعلومة حيزًا واسعًا في جريمة الابتزاز الالكتروني لذلك سنتطرق اليها باعتبار احدى ادواتها، لكونها اداة ضغط على الضحية فيما لو سخرها الجاني لصالحه.

وتعرف المعلومة بأنها (مجموعة من الرموز أو الحقائق أو المفاهيم او التعليمات التي تصلح لان تكون محلا للتبادل والاتصال أو التفسير أو التأويل أو المعالجة، التي تتم بواسطة الافراد والانظمة الالكترونية)،، ومن مميزات المعلومة انها محددة ومبتكرة وان تكون سرية،، ويعنى بالمحددة والمبتكرة ان تكون عبارة عن رموز او بيانات، واما سرية المعلومة يعنى بها انها غير متاحة للجميع، كمعلومة بحث علمي او معلومة خاصة بأمن دولة او...الخ، اما اذا كانت غير سرية فلا حماية عليها فيما يخص نشرها، ومثال ذلك ما تم ذكره في قرار سابق بالرقم(٨٩٩ و ٩١١ لسنة ٢٠١٧)بالجلسة رقم(٢١٩)بتاريخ ٢٠١٧/١٢/١٧ إذ كان اتاحة الصور الى الجميع ، كان سببًا بالحكم بعدم اعتداء المتهم على خصوصية المشتكي،.

اما المشرع العراقي فقد عرفها بأنها ((البيانات والنصوص والصور والاشكال والاصوات والرموز وقواعد البيانات وبرامج الحاسوب وما شابه ذلك التي تنشأ او تخزن او تعالج او ترسل بالوسائل الالكترونية))،.

اما مشروع قانون مكافحة الجرائم الالكترونية العراقي لسنة ٢٠١٩، فلم يتطرق الى مصطلح معلومة، فقد قسمها في المادة (١) منه الى محتوى وبيانات، وعرف المحتوى بأنه ((محتوى المادة الالكترونية أياً كان شكل المحتوى فيها نصاً أو صورة أو صوتاً أو فيديو وما في حكمها))، اما البيانات

فعرفها بأنها ((الارقام والحروف والرموز والاشكال والاصوات والصور وكل ما يتم تخزينه ومعالجته وتوليده وإنتاجه ونقلة بالحاسوب او اية وسائط الكترونية اخرى)).

اما التشريعات المقارنة فقد عرفها المشرع الاردني بأنها ((البيانات التي تم معالجتها واصبح لها دلالة))،، وقد ذكر تعريف البيانات الى جانب المعلومة في ذات المادة.

اما المشرع المصري فقد جاء بعبارة (البيانات والمعلومات الالكترونية)، وايضا تطرق في ذات المادة الى البيانات الشخصية والبيانات الحكومية،.

اما المشرع الاماراتي فقد كان تعريفه قريبا الى المشرع العراقي إذ عرفها بأنها ((أي معلومات يمكن تخزينها ومعالجتها وتوليدها ونقلها بوسائل تقنية المعلومات وبوجه خاص الكتابة والصور والصوت والأرقام والحروف والرموز والإشارات وغيرها))،.

اما الاتفاقية العربية الخاصة بمكافحة الجرائم المعلوماتية الصادرة سنة ٢٠١٣، فلم تتطرق الى مصطلح المعلومة بل تطرقت الى البيانات في المادة (الثانية/٣) وعرفتها بأنها ((كل ما يمكن تخزينه ومعالجته وتوليده ونقله بواسطة تقنية المعلومات، كالأرقام والحروف والرموز وما اليها...)).

والمعلومة في جريمة الابتزاز الالكتروني يمكن ان يحصل عليها الجاني من خارج الفضاء الالكتروني بحكم المعرفة او القرابة او الصدفة او الى غير ذلك من الطرق التي من خلالها تقع معلومات ذات اعتبار لدى شخص معين، مما يؤدي الى استغلاله لتلك الثغرة والضغط على الاخرين عن طريق وسيلة الكترونية وابتزازهم للحصول على منافع معينة، ويمكن ان تكون عن طريق الشبكة المعلوماتية اما عن طريق الثقة او الاحتيال او عن طريق السرقة واختراق خصوصية الاخرين والحصول عليها، فلولا المعلومة التي يحصل عليها الجاني فلا يمكن له ان ينفذ جريمته وان كان الجاني لا يمتلك معلومة ويهدد شخصًا اخر بحكم ان من يقوم بابتزازه شخص ضعيف الشخصية، فهنا ان علمه بأن هذا الشخص ضعيف الشخصية هي المعلومة بحد ذاتها وهذا وجهة نظر الباحث تقبل الصواب او الخطأ.