جريمة الابتزاز الالكتروني وطرق إثباتها في النظام السعودي (دراسة مقارنة)

الملخص العربي

جريمة الإبتزاز الإلكتروني وطرق إثباتها في النظام السعودي (دراسة مقارنة) إعداد الطالبة :شيماء وليد صدقة مرداد إشراف :أ.د. ماجدة فؤاد محمود مصطفى المستخلص بالرغم من المحاسن التي نجنيها من إستخدام الحاسب الآلي والإنترنت , إلا أن هنالك جانب سيء لهذا الإستخدام يتمثل في ظهور ظاهرة إجرامية تسمى بالجرائم المعلوماتية ,وبما أن جريمة الإبتزاز الإلكتروني تعتبر من اكثر الجرائم الإلكترونية انتشارا وضررا على الفرد والمجتمع مع صعوبة الحصول على آثار الجريمة بعد وقوعها نتيجة سهولة تخلص الجاني منها . لذلك كان من الواجب البحث في جريمة الإبتزاز الإلكتروني وطرق إثباتها في النظام السعودي والقانون المقارن , كما تهدف هذه الدراسة إلى بيان مفهوم جريمة الابتزاز الإلكتروني , مع بيان أنواعها وأركانها وخصائصها وماهي العقوبة المقررة لها وأخيرا بيان طرق إثبات هذه الجريمة بالوسائل التقليدية والحديثة , وتنقسم هذه الدراسة إلى فصلين , تضمن الفصل الأول بيان ماهية جريمة الإبتزاز الإلكتروني وأركانها , أما الفصل الثاني فتضمن طرق إثبات جريمة الإبتزاز الإلكتروني والتي تساعد في سرعة الوصول إلى الجاني ,ولقد توصلت الباحثة إلى عدة نتائج منها أن للمجرم الإلكتروني دوافع معينة وعديدة يسعى لتحقيقها , وان الباعث الغالب في جريمة الإبتزاز الإلكتروني هو الحصول على النفع المادي السريع , كما أننا نجد أن المنظم السعودي والمشرع الإماراتي قد نصا على عقوبة المبتز في جريمة الإبتزاز الإلكتروني بالحبس أو الغرامة أو بهما معا , وتعتبر الأدلة الرقمية هي أدلة مستحدثة جاءت لإثبات الجرائم الإلكترونية , وقد تكون هذه الأدلة في

الأصل أعدت لتكون وسيلة إثبات , وبتتبع النظام السعودي والقانون الإماراتي نجد انهما قد أخذا بالدليل الرقمي في الإثبات الجنائي, وفيما يتعلق بأهم توصيات الدراسة فتوصي الباحثة بان يكون هنالك تنسيق وتعاون بين مختلف الدول لمواجهة الجرائم الإلكترونية بشكل عام و جريمة الإبتزاز الإلكتروني بشكل خاص , مع وجوب المتابعة المستمرة لآخر ما يتوصل اليه خبراء الأمن المعلوماتي من الوسائل الفنية لحماية أمن المعلومات.

MEANS OF PROOF IN THE CRIME OF ELECTRONIC EXTORTION IN THE SAUDI SYSTEM (A COMPARATIVE STUDY)

Abstract

The crime of electronic blackmail and ways to prove it in the Saudi system (A COMPARATIVE STUDY) Prepared by: shimaa waleed sadagah merdad Supervised by: D. majda fuad Mahmoud Mustafa Abstract In Despite of the technical advantages of the use of Internet, it also imposes many disadvantages one of the main is the emergence of a criminal phenomenon called information crimes. Since the crime of cyber, blackmail is considered one of the most widespread dangerous cybercrimes, which poses a threat to the individual and society due to the difficulty of capturing legal evidence of the crime and how easy for offenders to dispose it. Therefore, it was necessary to study the crime of cyber blackmail and its evidence collection methods, this study aims to clarify the concept of cyber blackmailing by showcasing its types, pillars, and characteristics as well as its penalty. Includes studying the modern and traditional methods of proof in this specific crime. This study is divided into two chapters, the first included is an introductory chapter that studies the nature of cyber black mailing, and its characteristic. The second chapter examines the cyber blackmailing methods. The researcher has concluded the following conclusions, that the cybercriminal has specific and many motives that he seeks to achieve, and that the predominant motive in the crime of cyber blackmailing is to obtain quick financial benefit. Hence, the Saudi regulator and the UAE legislator have stipulated the punishment of the blackmailer in the crime of electronic extortion by imprisonment or a fine or both. The digital evidence is

considered the new evidence of cybercrimes. And by following the Saudi and UAE law, we find that they taken digital evidence as a legitimate criminal proof. The researcher recommends that there be coordination and cooperation between different countries to face cybercrimes in general and the crime of cyber blackmailing in particular, as well as the continuous follow-up to th