CiberData. Núm. 1, 2025, pp. 15-18

POSIBLES MODELOS DE REGULACIÓN DEL HACKTIVISMO ÉTICO EN LA LEGISLACIÓN ESPAÑOLA

Dra. María José Rodríguez Mesa
Universidad de Cádiz - España
Orcid: 0000-0003-4977-9978

Resumen. El hacking ético implica acceder sin autorización a sistemas informáticos con finalidad preventiva, lo que plantea dudas sobre su encaje penal cuando falta consentimiento. Si el bien jurídico protegido es la intimidad, el hacktivismo ético quedaría excluido; si lo es la seguridad de los sistemas, podría exceptuarse. El trabajo analiza la compatibilidad de los modelos bug bounty y CVD con el art. 197 bis CP y propone dos vías regulatorias: exigir dolo específico o introducir una exención penal ligada a protocolos CVD.
Palabras clave. Hacktivismo ético, Intrusismo informático, Seguridad de los sistemas, Bug bounty

Abstract. Ethical hacking involves unauthorized system access for preventive purposes, raising questions about criminal liability when consent is absent. If the protected legal interest is privacy, ethical hacktivism would be excluded; if it is system security, exceptions may be justified. This paper examines the compatibility of bug bounty and CVD models with Article 197 bis of the Spanish Criminal Code and proposes two regulatory approaches: requiring specific criminal intent or introducing an exemption linked to CVD protocols.
Keywords. Ethical hacktivism, Unauthorized computer access, System security, Bug bounty

Cómo citar: Rodríguez Mesa, María José (2025). "Posibles modelos de regulación del hacktivismo ético en la legislación española". En CiberData, núm. 1, 2025, pp. 15-18. Disponible en:

El calificativo de ético no neutraliza el hecho de que la conducta nuclear del hacking consista en acceder a un sistema informático vulnerando las medidas de seguridad establecidas originariamente. Esto es, acceder a una red en la que se almacenan y/o circulan datos de naturaleza heterogénea. Dichos datos pueden ser propios de una empresa, como por ejemplo patentes o cartera de clientes, o de un particular; públicos o privados; personales o no personales; etc.

El hacking ético solo se diferencia del hacking "negro" en su finalidad: en el primer caso para alertar sobre posibles fallos o brechas de seguridad; y en el segundo para cualquier otra finalidad que no sea la mencionada, incluida la consistente en el "mero fisgoneo".

La cuestión que plantea, por tanto, la decisión de legalizar o no el hacking ético es si es suficiente con que se pruebe el elemento subjetivo que lo define, o, en el caso de que la intromisión en el sistema no esté debidamente autorizada por el titular del mismo, el hackeo ha de estar jurídico-penalmente prohibido.

Si se considera que el bien jurídico protegido en el delito de intrusismo informático es la intimidad personal, el hacktivismo ético quedaría excluido del ordenamiento jurídico español, pues en aquellos casos en los que el sistema de información contenga base de datos de terceros, sería precisa la autorización de cada uno de éstos para el acceso al sistema informático. Si es la intimidad personal el bien jurídico vulnerado, tendrán que ser los titulares de los datos, y no el titular del sistema, el que preste la debida autorización.

Es cierto que en la actualidad este problema queda diluido en gran medida debido a las cláusulas genéricas sobre protección de datos en los que de forma previa se autoriza a la compañía al acceso de los datos, y en consecuencia a su autorización para el acceso por parte de un tercero. En estos casos no habría problemas en aquellos casos en los que el acceso se lleva a cabo por parte del personal contratado autorizado para detectar vulnerabilidades o fallas en el sistema. Mayores problemas pueden plantear los modelos de bug bounty o recompensas, y sobre todo el modelo de CVD.

Con respecto al bug bounty, son varias las empresas que ofertan sus servicios en España. Así, por ejemplo, la plataforma de bug bounty en español DragonJar es un servicio que se encarga de hacer la mediación entre los investigadores de seguridad y las empresas que deciden sacar su programa de recompensas. La plataforma cumple exclusivamente un servicio de mediación, pues el contrato se firma entre la empresa u organización y una comunidad de hackers éticos a fin de que éstos detecten las posibles vulnerabilidades en los sistemas y redes de la empresa. Una vez detectadas las vulnerabilidades se comunican a las empresas para que tomen las medidas necesarias y eviten ataques en el futuro. El valor de la recompensa va a depender de la gravedad de la vulnerabilidad que se haya encontrado.

Si se admite que el acceso debe ser autorizado por la empresa u organismo titular del sistema de información y no por los terceros titulares de los datos, el contrato de la empresa con la comunidad de hackers es ya autorización suficiente para que la conducta no sea típica, por lo que se trata de un modelo compatible con la actual regulación.

A diferencia de lo que ocurre en otros países, en España la Administración Pública no recurre a este tipo de programas, lo que implica que las vulnerabilidades solo puedan ser descubiertas por parte de los empleados o funcionarios encargados de la seguridad de los sistemas. Es de destacar, en este ámbito la experiencia piloto llevada a cabo por la Generalitat de Catalunya que invitó a 15 hackers para llevar a cabo el primer bug bounty de una Administración pública en España. La finalidad, además de la identificar vulnerabilidades en los sistemas de información y prevención de futuros ataques, era la de valorar las posibilidades y riesgos de este tipo programas en el ámbito de la Administración. A pesar del éxito del programa, en el que los hackers colaboraron desinteresadamente, son muchos los

aspectos, principalmente administrativos, que habría que regular para que los programas de bug bounty mediante recompensa pudieran convertirse en una alternativa viable en la Administración Pública.

La rigidez de la normativa sobre contratación de la Administración Pública (oferta pública, delimitación de tareas, precio, determinación de la parte contratista, etc.) es incompatible con la indeterminación de un modelo de bug bounty basado en una recompensa al hacker que detecte la vulnerabilidad cuya cuantía no viene establecida previamente, sino que depende de la gravedad de la vulnerabilidad detectada. Sería preciso, por una parte, crear un tipo de contrato administrativo adecuado a las particularidades del bug bounty; y, por otra, establecer una serie límites, compromisos y prohibiciones a los hackers que participen en el programa, pues no hay que olvidar que se les está dando acceso a sistemas informáticos públicos con datos sensibles y confidenciales, e incluso puede tratarse de sistemas informáticos pertenecientes a infraestructuras críticas.

Por último, y en cuanto a los programas CVD, España es uno de los países que ni siquiera se ha planteado su aplicación. Es más, con la actual redacción del art. 197 bis CP en la que el mero acceso no autorizado es delito, la comunicación de una vulnerabilidad grave por parte de un hacker ético a una empresa u organismo público sería la prueba del acceso ilícito, y por tanto de la comisión del delito. Ello implica que las vulnerabilidades detectadas por los hackers éticos no sean comunicadas o lo sean de forma anónima.

La implantación de un modelo de CVD en España como ocurre en países bajos, EEUU o Japón, exigiría en primer lugar una modificación de la tipificación vigente que, conforme a la posibilidad que deja abierta tanto el Convenio de Budapest como la Directiva 2014/40/UE, eximiera de responsabilidad penal a los hackers éticos que comuniquen la vulnerabilidad detectada.

No obstante, y antes de analizar los posibles modelos de exención penal, es preciso destacar que ello solo es posible si se admite que el bien jurídico protegido en este delito es la seguridad de los sistemas informáticos y no la intimidad personal ni la privacy. Y ello, porque tanto la intimidad personal como la privacy serían objeto de lesión con el mero acceso no autorizado, y ello con independencia de cuál sea la intención del sujeto activo. Ahora bien, si se entiende que el bien jurídico protegido es la seguridad de los sistemas informáticos, concretado en el caso del art. 197 bis CP en la confidencialidad de los sistemas, aquellas conductas dirigidas a potenciar la seguridad del sistema o de parte del mismo detectando y comunicando posibles vulnerabilidades, no lesionan, sino que contribuyen a la protección del bien jurídico seguridad de los sistemas informáticos, al proteger la confidencialidad de los mismos frente a posibles intromisiones ilícitas.

De considerarse éste el bien jurídico protegido, las alternativas para eximir de responsabilidad penal al hacker ético que actúe amparado por un modelo de CVD son principalmente dos: exigir como elemento subjetivo distinto del dolo la intención de obtener datos u otra intención delictiva; o incluir una cláusula de exención de la responsabilidad penal en aquellos casos en los que se comunique la vulnerabilidad conforme a los protocolos establecidos.

De ambas alternativas, la primera no exige una regulación previa del modelo de CVD, pues la simple ausencia del elemento subjetivo impide que la conducta sea típica. No obstante, y a pesar de ser una solución más simple y que no contradice al Convenio ni a la Directiva, se estaría destipificando el

"snooping" o fisgoneo no autorizado de los sistemas.

La segunda alternativa, exige tener previamente un protocolo de CVD, y solo eximiría de responsabilidad penal a quienes detecten y comuniquen la vulnerabilidad conforme al protocolo establecido. La exención, que habría de configurarse como una norma penal en blanco respecto al protocolo CVD, encontraría su fundamento en la ausencia de lesión o puesta en peligro del bien jurídico protegido: la seguridad de los sistemas informáticos.

La adopción de una política CVD incrementa la seguridad de las organizaciones, aunque ello también significa que la organización debe ser capaz de responder a la vulnerabilidad detectada. Una vez implantado en un Estado la política CVD, cualquier organización puede recibir un informe de vulnerabilidad. Sin embargo, cuando no existe una política CVD los reportadores de vulnerabilidades no tienen claro cómo responderá la organización, e incluso si su conducta pudiera ser perseguida como delito, por lo que la reacción esperada de la organización puede influir en el comportamiento de un posible divulgador. Una organización que no está respaldada por una política de CVD puede, por ejemplo, no saber cómo responder o no entender la vulnerabilidad y, por lo tanto, podría decidir ignorarla o negar la existencia de la vulnerabilidad. Incluso pueden malinterpretar las intenciones del divulgador y denunciarlo a la policía.