“LOS DELITOS INFORMÁTICOS EN LA DOCENCIA DE CIENCIA POLÍTICA A TRAVÉS DE MANIFESTACIONES CULTURALES”

NURIA MONTECELO CARBALLO
(UNIVERSIDAD DE VIGO)

XIV CONGRESO AECPA: CIENCIA POLÍTICA EN LA NUEVA POLÍTICA
DEL 10 AL 12 DE JULIO DE 2019. UNIVERSIDAD DE SALAMANCA
jueves, 11 de julio de 2019. 15:30 a 16:45 Lugar: 007B

Resumen: Los delitos informáticos e incluso ilícitos penales relacionados con las nuevas tecnologías, y las políticas públicas para su prevención y sanción, tales como la suplantación de identidad, forman parte de la enseñanza en ciencia política y derecho. En primer lugar, ponen en vilo la protección de aspectos importantes relacionados con el mundo de las artes, de las ciencias, del teatro, del cómic, de la literatura, de la pintura entre otras manifestaciones culturales. Asimismo, se evidencian preguntas que giran en torno a la falta de información de los ciudadanos y la vulneración de los derechos fundamentales; ¿hasta dónde llega el acceso al derecho a la información sin invadir ámbitos privados? ¿Cómo proteger derechos tan fundamentales como los derechos regulados en nuestra Constitución? Asimismo, se aportarán ejemplos de innovación docente en la enseñanza de estas cuestiones, a través de numerosas manifestaciones culturales.

Palabras clave: delitos informáticos, ciencia política, manifestaciones culturales, docencia

Introducción.

Los delitos informáticos e incluso ilícitos penales que, aunque no estén regulados todavía en nuestra legislación, hace obligado la realización de investigaciones y estudios, así como reflexiones. Un ejemplo es la suplantación de identidad a través de las redes sociales. Desgraciadamente, es uno de los múltiples hechos que en la era cibernética que nos rodea, puede acometerse, donde las redes sociales son frágiles ante la vulneración de nuevas conductas que hacen que la protección a derechos tan importantes como el derecho a la intimidad, derechos civiles, y aparentemente sin gran dificultad.

Es indudable que cada vez más, nos encontramos en una sociedad de riesgo, más vulnerable ante la presencia del ciberterrorismo y amenazas cibernéticas. ¿Hasta dónde llega el acceso al derecho a la información sin invadir ámbitos privados? ¿Cómo proteger derechos tan fundamentales como el derecho al honor (entre otros) regulado en nuestra Carta Magna? ¿Cómo protegernos del hecho de que cada día es más frecuente que suplanten nuestras identidades, utilizando nuestros nombres artísticos, obras literarias, pictóricas con absoluta impunidad?

En este breve trabajo se realizará un análisis que trate de profundizar y reflexionar desde una perspectiva desde el ámbito jurídico-social humanístico en cuanto a cómo pueden afectar a nuestra vida los delitos informáticos, y también metodologías y herramientas a utilizar para explicar estas cuestiones a través de numerosos ejemplos de manifestaciones culturales.

Los delitos informáticos.

La Orden PCI/ 487/2019 de 26 de abril del año 2019, por la que se publica la Estrategia Nacional de Ciberseguridad, regula la problemática y riesgos que entraña la Ciberseguridad. Al respecto en la era digital en la que estamos las actividades realizadas a través de las redes proliferan a un ritmo vertiginoso. En este sentido, ¿hasta dónde se encuentra protegida nuestra propia identidad virtual? Nuestra identidad "*online"* se une con la identidad *offline* (Burgueño, 2011: 125 y 127), y a consecuencia de las nuevas tecnologías estamos expuestos a intromisiones profesionales y también personales, una "mezcla" de lo que cada uno de nosotros queremos mostrar al exterior y que conscientes o no por el uso de las tecnologías y sin la protección o información debidas, somos o podemos ser víctimas de un ataque contra nuestra identidad y seguridad personal.

¿Somos al respecto conscientes del riesgo que entraña nuestras acciones dentro de Internet? ¿Quién establece los límites legales del derecho de intromisión a nuestra *privacy* (Hernandez, 2009:23)? No olvidemos que cada paso que dejamos en las redes, deja una huella difícil de borrar, expuesta a terceras personas con finalidades diversas, las cuales puedan derivar en que terceras personas sin nuestro consentimiento puedan utilizar y apropiarse de nuestros datos, abusando de nuestra identidad, de todos aquellos datos que dejamos almacenados y cuyo destino una vez en el ciberespacio es desconocido, y quizás muchas veces aprovechado por hackers, crackers o incluso con personas que aún no contando con una formación específica informáticamente hablando, sino que sólo con tener acceso a Internet, puedan utilizar nuestras identidades, nuestras claves, nuestros datos para atentar contra delitos tan importantes como el delito contra la intimidad, el honor, contra la libertad y la integridad moral (coacciones, amenazas) en definitiva, tan preciados y protegidos por nuestra Constitución, así como también de gran relevancia respecto de la Seguridad Pública (ciudadanos, gobiernos), y en definitiva, para los Estados.

Ahora bien, ¿existe el concepto de delito informático cómo tal? ¿Se debe de hablar de *delitos informáticos* (Hernandez, 2009:235), delincuencia informática cometida a través de un ordenador, delincuencia relacionada con el ordenador, o delincuencia a través de las nuevas tecnologías? Todavía no se regula un propio título en el Código penal que se denomine:" De los Delitos Informáticos". Estamos pues ante delitos o ilícitos penales de carácter pluriofensivo, no pudiendo determinarse una única acción comisiva ni un único objeto de delito, ni asimismo un único perfil de delincuente, si bien, parece ser que los delitos tienen como factor común que su comisión se realiza a través de un ordenador o bien, como ya se regula en nuestro código penal en el artículo 248.2 *estafa informática* (Faraldo, 2007:34), a través de un medio o artificio semejante. Al respecto, debido al avance de las Tics, así como un uso indebido de la información, los propios protagonistas y sujetos pasivos de estas conductas podrían ser los Gobiernos, Administración Públicas, Organismos Internacionales, Empresas Multinacionales que debieran plantearse si están sujetas a un suficiente "*seguridad informática"* (Hernández, 2009: 237).

Es ya de sobra conocido, que las conductas que se realizan a través de los ordenadores pueden vestirse a través de diferentes disfraces, bien sea espionaje profesional para beneficio personal o profesional, acceso a través de claves suplantando la identidad de las personas sin su consentimiento, o bien sea adquiriendo información a través del hardware o software de los ordenadores. De esta forma, el delincuente informático accede a los contenidos, apropiándose los mismos, cometiendo conductas que se encajan en figuras como el hurto el robo, la apropiación indebida, y fundamentalmente la estafa a través de Internet. Claro ejemplo de esto sería el "*phising"* (Kirda y Kruegel, 2006), o *"estafa informática"* (Faraldo, 2011;42) en donde los autores materiales de este delito envían un correo electrónico a particulares, haciéndose

pasar por directivos, solicitando claves de clientes para de esta forma acceder a la cuenta de los mismos, y así defraudar su patrimonio. Por otra parte, en el fraude al Ceo, se suplanta la identidad de un directivo de una empresa y mediante sus credenciales se tiene acceso a numerosa información tanto empresarial como personal.

Ahora bien, el problema que se plantea a la hora de enjuiciar estos delitos o ilícitos penales o civiles, además de ya no sólo una omisión en nuestro Derecho Penal e Internacional en cuanto a su regulación punitiva o en los supuestos en los que, si se regulan las conductas, las mismas, se encuentran en entredicho por las diversas legislaciones aplicables dependiendo de los países en los que se cometan. Se plantea en este sentido, la duda que genera la Jurisdicción o Tribunal competente que deba de conocer de su causa. Es sabido, que estas conductas se comenten en diferentes países, con nacionales o no nacionales de esos países miembros, involucrando a un único país o a varios de los mismos, dentro de la Unión Europea y fuera de la misma, entonces, ¿cuál debe de ser el Tribunal competente para conocer de estas causas? Al respecto, y siguiendo con la opinión de la Doctrina Jurisprudencial, la teoría de la acción y el resultado, la teoría de la ubicuidad, manifiestan interrogantes de cara a la Jurisdicción aplicable, ya no entremos a valorar cuando los daños se producen en un tercer Estado, es decir en un Estado en tránsito. La transnacionalidad de estos delitos, así como el anonimato de los sujetos activos de los mismos en internet, dificultan su persecución.

Es cierto que se ha avanzado considerablemente a nivel estatal y europeo en la regulación de estas conductas y en *seguridad en Internet* (Camenish, 2009) a través de las redes sociales, existiendo en nuestro país la Fiscalía de Delincuencia Informática, así como avances a nivel de investigación y persecución de estas conductas, mediante la creación de unidades especializadas dentro del marco de las Fuerzas y Cuerpos de Seguridad del Estado, sin embargo, no debe caer en el olvido que la era de la informática va por delante de las investigaciones, por lo tanto, es importante prevenir cada uno de nosotros como marca individual de nuestras direcciones personales en el ciberespacio, nuestros accesos a Internet, y nuestros perfiles o nicks en las Redes Sociales.

Sería idóneo avanzar más equitativamente en progreso de una sociedad más justa, en donde nuestros entornos físicos en el *ciberespacio* (Convenio Budapest sobre Ciberdelincuencia, 2001) se encuentren protegidos ante sorpresas informáticas, ante suplantaciones de identidad, que a día de hoy y por increíble que parezca estas conductas no se encuentran penadas. El principio "*non bis in ídem*", por muy insólito que parezca, no se cumple, porque existen ilícitos o conductas que pudiesen ser reprochable y que ni tan siquiera son reguladas por el Derecho Administrativo. El principio de intervención mínima del Estado no se cumple, ni administrativamente se persiguen, por lo tanto, surgen la necesidad de realizar propuestas de *lege ferenda*, y colmar los vacíos legales por el legislador[1].

La denominada "*generación de Internet"*, avanza a pasos agigantados, ante unas instituciones que necesitan avanzar con más agilidad para prevenir conductas que atenten contra el material tan preciado como es su información. La criminalidad a través de "*las tecnologías de la información"* (Rayón, 2006:214), de la informática y de sus medios, necesita más avances y progresos. Todos nosotros somos responsables de nuestras conductas en las redes, pero ello no es suficiente ni es justificación para que no se regulen estas nuevas figuras, acorde con una legislación más adecuada y al día con los avances tecnológicos. El Consejo Nacional de Seguridad Nacional, ya aprobó en reunión de 12 de abril de 2019, la Estrategia Nacional de

[1] La suplantación de identidad se distingue de la conducta regulada en el artículo 401 del código penal, que regula la usurpación del estado civil pero que, a diferencia de la suplantación de identidad, usurpan todas las facetas de nuestra vida no sólo en las redes sociales.

Ciberseguridad, un avance muy significativo para prevenir amenazas que surgen en el ciberespacio dentro del marco de Política de Seguridad del Estado. A nivel europeo, el Convenio de Budapest tiene como objetivos prioritarios combatir la ciberdelincuencia, armonizando las diferentes legislaciones aplicables al derecho informático, agilizando los trámites procesales y jurisdiccionales, todo ello mediante un régimen dinámico de cooperación internacional.

Cabe mencionar algunos ejemplos de delitos informáticos relacionados con la suplantación de identidad*:* El "*Phishing"* (Kirda y Kruegel, 2006) consiste en suplantar la identidad de una persona con la finalidad de obtener información de tarjetas de crédito, débito, contraseñas, información de cuentas y otros datos. El llamado *"phisher",* quiere menoscabar el patrimonio de las víctimas, y lanza *"anzuelos"* (Gudin, 2009:3)*,* creando un link irreal de una entidad bancaria, para que de esta forma las víctimas accedan a su contenido y a la petición de poner sus propias claves. Otra de las modalidades que utilizan es "spear phising" o caza con lanza (Gudin, 2009:3) consistente en enviar correos electrónicos a sus víctimas, solicitando claves de acceso, número de cuentas bancarias, o cualquier otro dato de interés para poder menoscabar el patrimonio de las mismas. En otros casos, les envían correos electrónicos engañosos, se les hace creer que han sido ganadores de algún premio de lotería, pero deben de facilitar datos personales para conseguir lo prometido.

La conducta de "*Pharming"* (Gudin, 2009:4) consiste en explotar la vulnerabilidad en el software de los servidores DNS o en equipos de los propios usuarios, es decir, se explota la vulnerabilidad de los servidores DNS o de equipos de usuarios para de esta forma redirigir un dominio a otro ordenador. Siguiendo con lo explicado por el mismo autor, mediante las acciones de Skimming y Scamming los sujetos activos de estos delitos duplican nuestras tarjetas, mediante unos dispositivos que insertan cuidadosamente en los cajeros automáticos. Una vez se introduce la tarjeta, el dispositivo hace que se clone una tarjeta igual con todas las características que nuestra tarjeta tiene.

En el "*Hacking*" *o intrusismo informático"* (Gudin, 2009; 7) se vulnera el derecho a la intimidad de otra persona, afecta por lo tanto a la más estricta confidencialidad y exclusividad de la información, derechos de propiedad intelectual, industrial y contra los secretos empresariales se ven afectados. Utilizan *bombas lógicas, caballos de troya o la denominada técnica del salami que provocan la realización automática de transferencias bancarias, ingresos o reconocimiento de créditos a favor de quien realiza la alteración (*Gudin, 2009; 8), y acceder a la información reservada y personal de sus víctimas. La diferencia entre el hacking y el cracking, consiste en que en el primero el sistema o la información no se deja inoperativo, si no lo que sucede es que se accede al contenido, pero el mismo no sufre ningún daño.

Las conductas ilícitas que se producen en las Redes Sociales a través la Suplantación de Identidad, lleva emparejada el ataque a bienes tan preciados como la protección al honor, intimidad y seguridad personales, amenazas, coacciones, injurias… Las personas que atentan en las Redes Sociales, la mayoría suelen crear perfiles falsos, suplantando nuestra identidad con datos veraces a cerca de nosotros mismos, pero creando una o varios perfiles como si de nosotros mismos se tratase, sin mediar nuestro consentimiento. En los delitos cometidos en las Redes Sociales, las Fuerzas y Cuerpos de Seguridad del Estado a nivel de investigación y persecución, destacan la relevancia práctica de las primeras actuaciones, destinadas a recoger de manera más fiel posible (física y tecnológicamente) los contenidos publicados en un momento dado antes de que desaparezca o modifique el rastro o huella en la web de la infracción penal: acreditación de atestado policial (acta, captura de pantalla..) intervención de fedatario público (Letrado Administración de Justicia o Notario) inspección ocular o reconocimiento judicial, o incluso con la intervención de empresas especializadas (prestadores de servicios de confianza) que contribuyen a acreditar que un contenido fue efectivamente

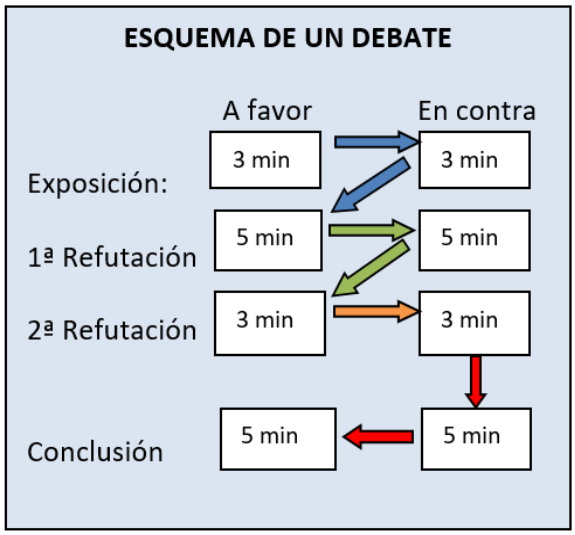
generado o publicado y que no ha sido modificado por el usuario. Existen ciertas aplicaciones o software que pueden determinar la preservación de contenidos online. De forma intuitiva y rellenando los campos facilitados, permiten certificar en tiempo y forma los contenidos web, email y otros documentos electrónicos.

Los delitos informáticos en la docencia de Ciencia Política y de la Administración a través de manifestaciones culturales.

Son numerosas las manifestaciones culturales que nos acerca al mundo específico de los delincuentes informáticos. De sobra conocidas, deben mencionarse películas como *"Hackers Piratas informáticos", "El Talento de Mr. Ripley", "Hackers a Gogó",* el documental *"Zero Days"* entre otras muchas manifestaciones las que nos van a servir como ejemplo para mostrar al alumnado ilícitos informáticos tan peculiares y a la vez tan reales en nuestros días. La diversidad es amplia, en este punto ya en el año 1995 la película *"Hackers Piratas Informáticos"* cuya protagonista es Angelina Jolie y Jhonie Lee Miller, nos adentraban al mundo de los hackers, y lo que parecía en su momento ciencia ficción como argumento de la mencionada película, hoy en día se convierte en una manifestación cultural que refleja la realidad de nuestros días.

Las infraestructuras críticas de los Estados se reinventan para tratar de controlar y prevenir conductas ilícitas que se desarrollan a través de las redes. Al respecto el protagonista Jonny Lee Miller, (Dade Murphy y con Nick Zero Cool) siendo un niño consigue que caigan más de 1500 sistemas en Wall Street lo que le lleva a que le castiguen sin poder tocar un ordenador hasta su mayoría de edad y que una vez en el instituto se encuentra con la protagonista Angelina Jolie (Kate Libby y Nick Acid Burn) y otros autores. Sus acciones se ven envueltas en una trama de hackers que descubren una estafa empresarial. A través de sus acciones en Internet, suplantan diversas identidades, crean pseudónimos para evitar ser descubiertos. Asimismo, se identifican como un movimiento punk, que le gustan los videojuegos y todo lo relacionado con los ordenadores, con un lenguaje propio en el que ellos mismos se consideran seres anónimos, y cuyas contraseñas son "amor" "secreto" "sexo" y "dios". Se encuentran inmersos en una estafa empresarial, en el cual un pirata informático crea un virus- gusano que debe infectar barcos dirigidos por satélites. Para analizar esta película haciendo partícipes al alumnado, puede utilizarse la herramienta didáctica del debate.

ESQUEMA DE LOS PASOS E INFORMACIÓN NECESARIA PARA PREPARAR A LOS ALUMNOS PARA EL DEBATE.
1.-Preparar a los estudiantes para el debate sobre un tema. **2.-Decidir la tesis a debatir.** **3.-Asignar los equipos de debate.** **4.-Orientar la estrategia del equipo.** **5.-Orientar la investigación y la construcción de la argumentación.** **6.- Dar instrucciones claras sobre la metodología del debate y las reglas a seguir.** **7.-Preparar los medios a través de los cuales se realizará el debate.** **8.- Definir el papel de la audiencia.** *** **9.- Moderar el debate.** **10.-Evaluar el proceso.**

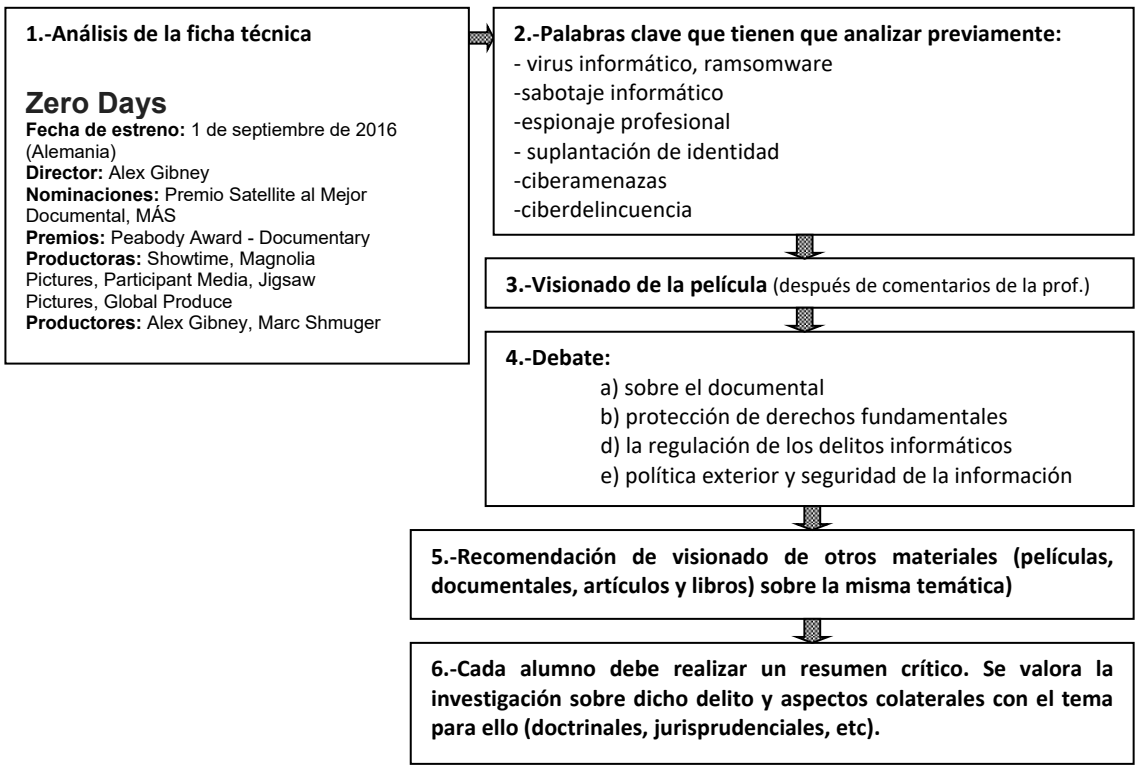


Para ello, es muy importante que el docente sepa elegir la información imprescindible con la que los alumnos deben contar para fijar sus conocimientos sobre las conductas que realiza un hacker. Para ello adjunto documentos, vídeos y power points. Asimismo, les muestro información sobre las reglas del debate y algunos consejos para una sólida argumentación (técnicas de argumentación jurídico-politológicas). Les formulo preguntas para entender las razones y argumentos detrás de cada punto de vista.

Les explico documental y gráficamente la diferencia, entre otros, de los discursos para informar respecto a los discursos para persuadir; la adaptación a la audiencia y al ambiente espacio-temporal; "construir hacia atrás", es decir: cómo cerrar un discurso; pautas inductivas y deductivas; el efecto de recencia; el paralenguaje; la Kinésica; la Proxémica, etcétera. A continuación, expongo un ejemplo-esquema debate que puede proponerse

Así también a modo de ejemplo de delincuencia informática, en el documental del autor Alex Gibney, *"Zero Days"* del año 2006, se centra en acciones ilícitas del aparato de guerra cibernética de los E.E.U.U. La trama gira en Beliorusia en donde se descubre un supervirus de una gran complejidad, cuya principal misión es entrar en los complejos subterráneos del enriquecimiento de uranio en Irán. Se quieren destruir las máquinas centrífugas para evitar que el estado iraní sea capaz de crear una bomba atómica. El virus llamado Stuxnet, se sabe que proviene de una agencia estadounidense cuyo propósito es interrumpir el programa atómico de Irán. Delitos de descubrimiento y revelación de secretos, espionaje profesional e industrial, suplantación de identidad entre otros se manifiestan en este documental que no ha pasado desapercibido al público y que a modo simbólico refleja la realidad oculta en torno al mundo de los denominados servicios de inteligencia, en este caso americanos e israelís y mediante el mismo se abre un debate sobre qué ocurriría si los Gobiernos no hacen pública sus intenciones en materia de guerra y política exterior. Con el estudio de este documental, aplico otra metodología diferente: didáctica del análisis de la película.

Ejemplo de práctica con un documental "Zero Days":



En películas de la saga *"Misión Imposible"* cuya andadura empieza en el año 1996 con el famoso autor Tom Cruise y director Brian de Palma, se adentra ya en el mundo de la nanotecnología, biometría… mediante técnicas de inteligencia artificial se hacían pasar unos autores por otros. Otro claro ejemplo de suplantación de identidad en toda regla llevado al límite más amplio imaginado. Reflexión… ¿Será que el cine y resto de manifestaciones culturales a modo de ciencia ficción- y no tanto ciencia ficción- van un paso por delante del avance social referente a los delitos informáticos?

Como pueden comprobar, a la hora de transmitir los conocimientos de delitos informáticos a los alumnos, he elegido películas que siendo de diferentes fechas, el guión de las mismas, encuadra con lo expuesto en las páginas anteriores relativas a los delitos informáticos (*hackivismo, crackers*, sabotaje informático, *phishing, pharming, skimming, skamming*, suplantación de identidades en las redes). También a través de la pintura, el cómic, la música, se pueden expresar y manifestar acciones relacionadas con los delitos informáticos. Por lo tanto, sus autores tienen una propia "*identidad cultural"* (Molano, 2007; 74), en la cual se retroalimentan de sus conocimientos, y con un lenguaje simbólico manifiestan un ánimo diverso, en unos casos su malestar social, en otros casos, su finalidad es ánimo de lucro tratando de comprar a los Estados o empresas multinacionales.

En la canción *"Nuevas Formas de Hacer el Ridículo*", de Carolina Durante, se relata como *"el perfil online supera a las personas"*. Como relata la propia canción, *"es como si se conociesen de toda la vida"* pero *"no lo suficiente"* La canción manifiesta la problemática de las redes sociales, y como una foto expuesta en una red social, puede generar conductas como las expuestas en la canción. Son ejemplos de manifestaciones culturales y sirven para mostrar a la sociedad y al público en general que estas conductas se manifiestan y están presentes como auténticas formas de vida que operan y se manifiestan. El sentimiento de identidad y continuidad está presente en los mismos lejos de negarse, deben de estar presente a través de un sentimiento de perdurabilidad.

Otros ejemplos que no entraré en profundidad a explicar los encontramos en películas como: "Suplantación de Identidad". En esta película estadounidense de 2013, una de las protagonistas (Heather) le pide a la alumna más aventajada de la clase que se haga pasar por ellas en el examen de ingreso en la universidad a cambio de dinero. La joven acepta porque su familia lo necesita sin embargo las cosas no salen como quieren y la alumna más aventajada llamada Meredith saca una mala nota en un examen tipo test, lo que se complica todavía aún más cuando Meredith aparece muerta y las tres chicas Heather, Kylie y Jordan se ven envueltas en toda una trama de acción y suspense. Se produce el ilícito penal de suplantación de identidad, en el cual una de las protagonistas se hace pasar por otra persona en un examen. En la película "La Ladrona de Identidades" (estadounidense, 2013), Diana roba la identidad de Sandy Patterson el cual comprueba como su vida económica, profesional se pone en peligro por culpa de Diana, residente en Florida, la cual lleva una vida lujosa y a la cual Sandy persigue para limpiar su propia reputación.

Asimismo, "Catch me if you Can" (EEUU, 2002), es una película que visibiliza delitos como la suplantación de identidad y la falsificación de documentos, concretamente de cheques bancarios. Su protagonista, Leonardo Di Capprio, suplanta la identidad de un piloto de avión, de un profesor y de un médico. Su profesionalidad a la hora de falsificar cheques bancarios es tal, que incluso el FBI le contrata como asesor en este tipo de fraudes. En la película "Face OFF" (EEUU, 1997, se suplanta la identidad de un peligroso terrorista que se encuentra en coma en un hospital. Los actores son John Travolta (Sean Archer agente del FBI) y Nicolage Cage (Castor Troy Peligroso Terrorista) Ambos se someten a operaciones de rostro, que les hacen cambiar por completo sus vidas, llegando incluso a usurpar el estado civil de Sean y Sean el de Castor Troy. En "Robo de Identidad" (canadiense, 2004), una empleada de una inmobiliaria suplanta la

identidad de una profesora llamada Michelle, comprando compulsivamente con su tarjeta de crédito, a la que el banco le acaba de conceder un crédito por la compra de una vivienda. La protagonista como víctima del fraude es Kimberly Williams (Hija de Steve Martins) y la impostora es (Michelle) la interpreta Annabella Sciorra. "The Big Lebowsky" (EEUU, 2013) es una película que se desarrolla en la ciudad de los Ángeles, cuyos protagonistas son tres amigos, Jefrey "The Dude", Walter Sobchak (Jonh Goodman) y Donny (Steve Buscemi) y el Sr Lewosky interpretada por David Huddleston. En esta ocasión The Dude suplanta la identidad del Sr Lewosky, otro ejemplo de suplantación de identidad reflejada en el cine.

La película titulada "Dead Ringers" (estadounidense-canadiense, 1998) narra la historia de dos gemelos idénticos, de profesión ginecólogos, especialistas en problemas de fertilización femenina. Elliot suplanta la identidad de su gemelo Beberly y se dedica a conquistar mujeres, una vez que se cansa de ellas, será su gemelo quien se haga pasar por Elliot. La película es un constante engaño de personalidades, hasta que ambos gemelos son descubiertos por una paciente Claire Niveau. El papel de los dos gemelos es realizado por Jeremy Irons. El principal argumento de "El Talento de Mr. Riplay" (estadounidense, 1999), interpretada por Matt Damon, es la historia de un joven empleado de una empresa de servicios de Manhattan Tom Ripley, que se hace pasar por un estudiante de la universidad de Princenton, y que recibe una suma elevada de dinero para convencer al hijo de un millonario que regrese a su hogar para dirigir la empresa familiar y pasar los últimos años con su madre la cual se encuentra en estado grave. Cuando conoce al hijo del millonario, Dicke comprueba que lleva un estilo de vida para el envidiable junto con su novia Marge (Gwyneth Paltrow).

Por poner un último ejemplo, en concreto de un documental, "Catfish" (estadounidense, 2010), se refleja otro caso donde las redes sociales, concretamente Facebook, es protagonista de esta historia. Una madre, Ángela, con serios problemas se hace pasar por su supuesta hija de tan solo ocho años de edad y contacta con un fotógrafo llamado Nev. Pronto Ángela suplantando la identidad de su joven hija le envía un cuadro de una de sus fotografías al domicilio de un fotógrafo Nev, creyendo Nev que se trata de un cuadro hecho por la hija de ocho años y no por Ángela. Ángela a su vez, suplanta la identidad de su familia, creando perfiles falsos en Facebook, lo que induce en error a Nev, creyendo la ficción que le cuenta Ángela a través de las redes sociales.

CONCLUSIONES.

La aplicación de las manifestaciones culturales en la enseñanza en Derecho y Ciencia Política es muy provechosa en la docencia universitaria para abordar temas y aspectos de la actualidad, tales como los delitos informáticos, haciendo especial hincapié en el delito de suplantación de identidad (como ejemplos en el presente trabajo). Es un enfoque distinto que permite conectar con una gran variedad de públicos, especialmente con los/as más jóvenes.

El alumnado desarrolla un notable interés por la asignatura, adquieren numerosos conocimientos y destrezas al buscar información relacionada con el caso que se les presenta, y permite desarrollar su espíritu crítico a la hora de observar, contrastar y refutar los contenidos de la materia con la propia actualidad, en muchas de las ocasiones mostrada a través de películas o documentales. En otras ocasiones, como cualquier otra realidad, es susceptible de valoraciones y subjetividades, y fomenta la utilización del debate, herramienta que he utilizado en alguno de los ejemplos señalados.

BIBLIOGRAFÍA.

FARALDO CABANA, P.: *Los conceptos de manipulación informática y artificio semejante en el delito de estafa informal,* 2007

HERNANDEZ DÍAZ, L.: *El delito informático,* 2007

RAYÓN BALLESTEROS, M.C Y GÓMEZ HERNÁNDEZ J.A.: *Cibercrimen: particularidades en su investigación y enjuiciamiento.* 2014

RICOY CASAS, R.: *La enseñanza de la Ciencia Política y el Derecho a través de las manifestaciones culturales contemporáneas*

GÓMEZ PERALS, M.: *Delitos informáticos en el Derecho Español*

GIONES VALLS, A Y SERRAT BRUSTENGA, M.: *La gestión de la identidad digital: nueva habilidad información y digital.* 2010

FERNANDEZ BURGUEÑO, P.: *Aspectos Jurídicos de la Identidad Digital y la reputación on-line*, 2011

ACUARIO DEL PINO, S.: *Delitos informáticos. Generalidades*

GUDIN RODRIGUEZ- MAGARIÑOS, F.: *Nuevos Delitos Informáticos, Phising, Pharming, Hacking, Cracking.* 2009

Convenio de Budapest, 2001

Orden PCI/487/2019 de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad v2019, aprobada por el Consejo de Seguridad Nacional.

MOLANO, L: *Identidad Cultural un concepto que evoluciona. Opera, 7, 7 (noviembre2007), 69-84*