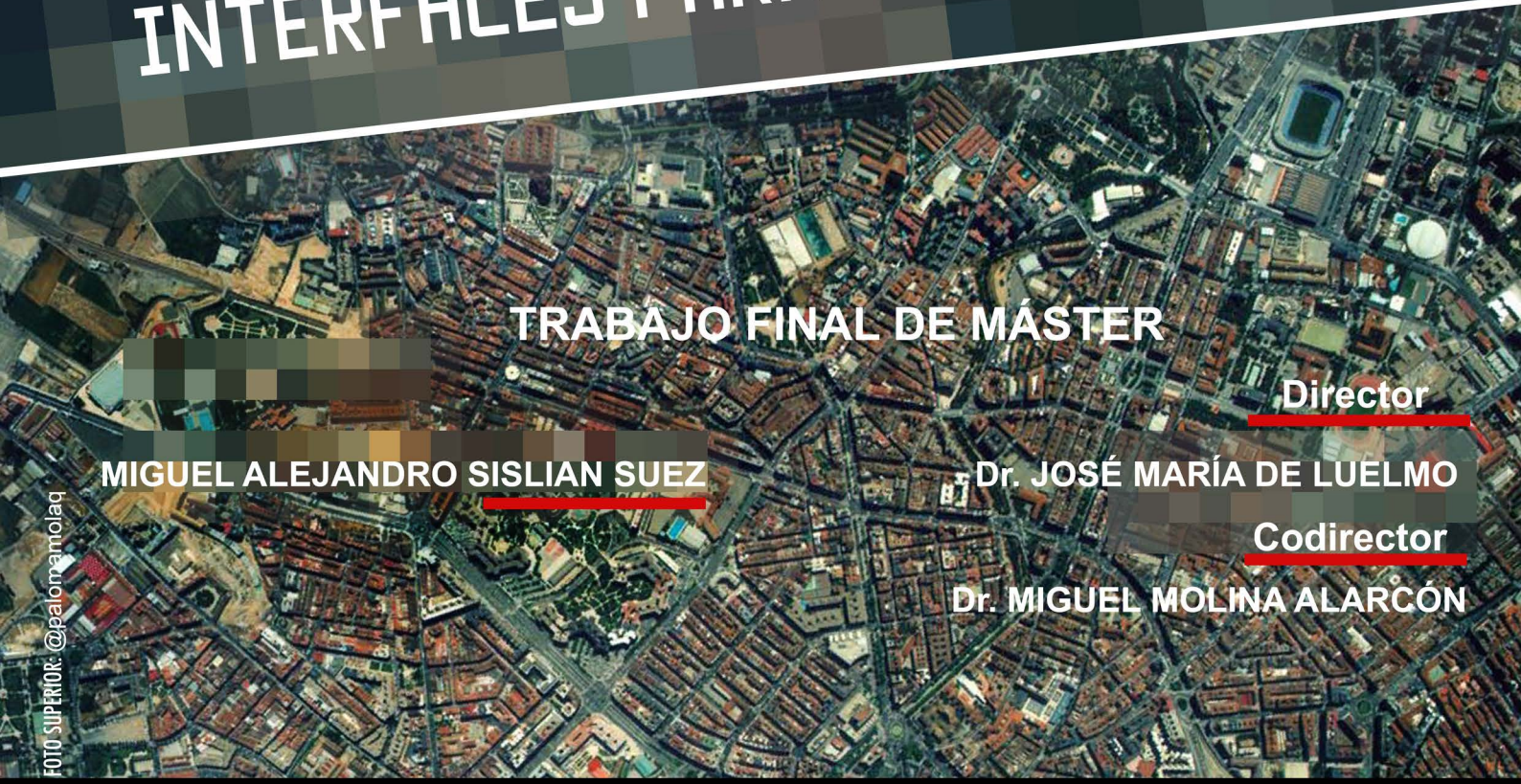
OFICIAL^PÚBLICO
MÁSTER
ARTES
VISUALES +
MULTIMEDIA

CONTRA

INTERFACES PARA LA RESISTENCIA



TRABAJO FINAL DE MÁSTER

[redacted]

MIGUEL ALEJANDRO SISLIAN SUEZ

Director

Dr. JOSÉ MARÍA DE LUELMO

Codirector

Dr. MIGUEL MOLINA ALARCÓN

FOTO SUPERIOR: @palomamolaq

UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Artes Visuales & Multimedia
Máster Oficial· UPV

MÁSTER UNIVERSITARIO
EN ARTES VISUALES Y MULTIMEDIA

TRABAJO FINAL DE MÁSTER

CONTRA
INTERFACES PARA LA RESISTENCIA

Trabajo presentado por:
Miguel Alejandro Sislian Suez

Dirigido por:
Dr. José María de Luelmo

Codirigido por:
Dr. Miguel Molina Alarcón

VALENCIA, julio 2019

AGRADECIMIENTOS

Gracias a mi madre por haber insistido todos estos años para que siguiese estudiando, aunque no fuese esto lo que ella imaginaba.

Quiero agradecer infinitamente el apoyo recibido por parte del profesorado de telecomunicaciones e informática a la hora de resolverme dudas y el cuidadoso interés mostrado por el proyecto. He de reconocer del mismo modo a Rubén Quintanilla por haber invertido su tiempo en darme clases de informática y haber estado en todo momento implicado, ya que sin su ayuda no hubiese podido resolver de manera óptima este proyecto.

Debo nombrar especialmente a José María de Luelmo por haberme dado tanta cancha a pesar de mis modos de proceder y aun así haber seguido ayudándome, a Miguel Molina Alarcón por ver siempre lo positivo de las cosas y a Marina Pastor Aguilar por prestarme su tiempo inexistente para tenderme una mano en horas bajas.

Quisiera también reconocer y agradecer la ayuda incondicional de mis amigos, en especial a Lucía Blas Vilaplana por aportarme dos ojos más en mi trabajo teórico, y a Alicia de la Fuente de los Ángeles (Dela Delos) por haberme ayudado a resolver mis carencias como sastre.

Resumen

CONTRA: Interfaces para la resistencia, se presenta como una interfaz de carácter crítico en relación con los sistemas del poder tanto físicos como digitales ejercidos sobre los individuos en las sociedades contemporáneas. ¿Cómo han evolucionado los dispositivos de control desde la aparición del alambre de espino? La investigación realizada abordará las relaciones y mecánicas empleadas sobre los individuos a partir del Absolutismo hasta las democracias liberales, y como estos dispositivos se han actualizado haciéndose inmanentes al individuo.

Palabras clave: poder, dispositivo, interfaz crítico, biopolítica, dispositivo de inmunidad

Abstract

CONTRA: Interfaces for resistance consists of an interface with a critical character in relation to both physical and digital power systems which control individuals in contemporary societies. How control devices evolutioned since barbed wire started to be used as one of them? Our research studies the relations and mechanicals used from Absolutism about individuals up to Liberal Democracies, taking into account the way these devices have been updated in order to become something inherent to individuals.

Key words: power, device, critical interface, biopolitics, immunity device

Índice

"Una dictadura universal con apariencia democrática,
una cárcel sin muros de la cual los prisioneros
no podrán ni soñar con evadirse […]
agradecidos por su situación de siervos."
(Huxley 2014, 5)

1. INTRODUCCIÓN

El presente trabajo final del Máster en Artes Visuales y Multimedia de la Universitat Politècnica de Valencia, titulado CONTRA: Interfaces para la resistencia, se adscribe dentro de dicho máster a las líneas de investigación en lenguajes audiovisuales y cultura social, estética digital, interacción y comportamientos, enmarcándose además en las subcategorías de resistencia, nuevos medios y diseño de interfaz.

Debemos señalar, ante todo, que el objeto de esta investigación ha sufrido mutaciones a lo largo del tiempo. En un principio giraba en torno al tema de los refugiados, buscando métodos de invisibilización para atravesar las fronteras y evitar la consecuente reclusión de masas, y de esta idea solo ha quedado la metáfora del dispositivo resultante, que no abandona en su totalidad su principal motivación: la invisibilidad. Las interfaces a los que aludimos en el título hacen referencia de manera concreta a dispositivos de cualquier índole que colaboren en la lucha para priorizar los derechos y la privacidad de los individuos en la era de los dispositivos digitales, y colateralmente en sistemas más analógicos. A partir de la interfaz que se ha confeccionado para esta investigación, que aunque metafórica es en su forma totalmente funcional, tratamos de promover la reflexión acerca de la importancia y la obligación de proteger tanto nuestra privacidad como la de los demás en un contexto de pérdida constante de las libertades individuales.

1.1. Estructura del documento

La investigación se divide en seis apartados interrelacionados. En el primer apartado se establecen el resumen global y las líneas de investigación en las que nos hemos posicionado, seguido de los objetivos y motivación para la realización del proyecto, así como la metodología seguida para desarrollar la investigación.

El segundo apartado se centra en la investigación conceptual y referencial, abordando la cuestión del poder y las mecánicas de control desde los regímenes absolutistas hasta las Democracias Liberales. Este apartado da paso al tercero, en el que se tratan el concepto de dispositivo de control, la aparición del alambre de espino como paradigma de ello y su evolución hacia los actuales sistemas de control digital, pasando por la teoría de lo liso y lo estriado de Deleuze y la vigilancia constante y su relación con lo cibernético. Se intercalan aquí teoría, casos actuales y prácticas artísticas, con la intención de ayudar a una mejor comprensión del tema y relacionar entre sí los elementos simbólicos utilizados para la propuesta artística.

En el cuarto apartado teorizaremos sobre el concepto Bio, haciendo una introducción esquemática a la biopolítica según Foucault, Agamben y Esposito, y dando paso al llamado biodispositivo para establecer así un mapa general de la cuestión. Cerraremos este bloque con una reflexión sobre la necesidad de reflexionar sobre las tecnologías y la urgencia de crear contra-dispositivos.

El quinto apartado arranca con la mención de algunos referentes artísticos que no se han incluido en el bloque teórico pero son necesarios para entender adecuadamente la propuesta. En este apartado se desglosa detenidamente la experimentación o práctica artística: planteamiento del proyecto, antecedentes, diagramas de interacción, materiales empleados, electrónica y diagramas de circuitos, etc., incluyendo abundantes imágenes del prototipo, de su exhibición en distintos espacios y de su comportamiento en el espacio público.

En el sexto y último apartado se establecen conclusiones y se plantean las futuras mejoras a aplicar al prototipo. Posteriormente se detallan todas las referencias empleadas en la investigación. Por motivos de extensión, todo el código de programación utilizado se incorpora como un link al repositorio de GitHub donde se encuentra todo lo realizado sobre los códigos Open Source.

1.2. Motivación y justificación de la investigación

CONTRA: interfaces para la resistencia es, por tanto, un proyecto que resulta de la unión entre arte y tecnología y del interés crítico por el control ejercido sobre los flujos migratorios, un control que se extrapola hoy en día a las ciudades contemporáneas y pone de manifiesto la necesidad de buscar los últimos reductos donde la privacidad y la invisibilidad se pueda seguir ejerciendo. En esta coyuntura, nuestra responsabilidad es buscar dispositivos de resistencia para la comunicación y el desarrollo colectivo de las sociedades y para inmunizarnos respecto a las nuevas estrategias de las redes del control, devolviéndonos de ese modo la soberanía de nuestra libertad individual y política.

Con ese fin, el trabajo parte de una indagación sobre los sistemas y dispositivos de control en las sociedades contemporáneas, entendiendo que en ellas se ha producido el cambio de sociedades disciplinarias definido por Foucault a las sociedades de control analizadas por Deleuze, donde cualquier individuo acepta por voluntad propia el hecho de ser vigilado incesantemente y en la que cualquier toma de decisiones viene mediada y modulada a partir de dispositivos físicos, psicológicos, visuales, etc. (Agamben 2015, 23). Para ello estableceremos una continuidad temporal que contextualice la problemática contemporánea en torno al poder, el comportamiento y significado de los dispositivos de vigilancia y su evolución, partiendo de los métodos coercitivos empleados en los Estados Absolutistas y llegando hasta lo que llamaremos biodispositivos, inscritos en el marco de las llamadas Democracias Liberales.

A la vista de todo ello, el posterior proceso creativo experimental conduce a un prototipo que consta de una interfaz física de tipo TUI (Tangible User Interface), que se presenta en un formato de wearable y que permite al usuario lograr la invisibilidad en términos cuantitativos en los espacios de las redes de comunicación. La idea de crear un wearable que permita este tipo de invisibilidad tiene como objeto invitar al usuario a ser participe de una reflexión activa sobre la dependencia de las sociedades con respecto a los sistemas virtuales de control y vigilancia, sistemas con los que actualmente convivimos de un modo inmanente. Esta circunstancia plantea la necesidad de buscar métodos de contra-vigilancia que nos ayuden a encontrar espacios difusos donde contraponernos con un carácter de resistencia y rebeldía al poder establecido, a ese régimen escópico omnipresente.

Quizá todo esto solo sirva para darnos cuenta de lo que caracteriza a esta época: un lugar en el que los dispositivos modulan totalmente nuestra subjetividad, abocándonos a ser una sociedad contemplativa y disciplinada que acepta el colapso de su existencia física para convertirse, en esencia, en un conjunto de datos cuantificables y comercializables sin restricciones. Lo que se establece en las próximas páginas es una reflexión sobre la perdida de derechos y la privacidad personal, un tema que actualmente ha ganado una gran presencia a nivel social y que, a título personal, me ha suscitado una cuestión práctica: ¿qué hacer para contraatacar o resistir ante los actuales sistemas de control?

1.3. Objetivos

Incidiendo en todo ello desde un posicionamiento directo y comprometido, el proyecto Contra se propone emplear la práctica artística para reflexionar sobre los nuevos dispositivos y mecánicas instituidas para ejercer el control y sobre la manera en que han evolucionado de lo físico a lo virtual. Para ello establecemos una serie de objetivos, de lo más general a lo más específico:

Generales

- Trazar un mapa sobre los mecanismos de control en la Modernidad.
- Establecer las variables fundamentales de la relación poder-individuo en la actualidad.
- Promover la reflexión crítica sobre las consecuencias del uso de dispositivos basados en la gestión de la privacidad.

Específicos

- Analizar los distintos dispositivos de control individual en la actualidad y diseñar un contradispositivo portátil de autoprotección digital.
- Producir un wearable que incite al usuario a reivindicar y participar activamente en la gestión de su privacidad.

1.4. Metodología

La metodología empleada para este proyecto de investigación ha dependido de las fases de desarrollo. Se inicia con una metodología principalmente deductiva, ya que parte de la teoría general socio-política característica de los Estados Absolutistas y de las Democracias Liberales. A esta fase sigue otra donde una metodología cualitativa y crítica sirve para efectuar un cuestionamiento de los sistemas de poder y las necesidades creadas en torno a las nuevas tecnologías y la sobreexposición a los mecanismos de control derivados de ellas.

A toda esta investigación conceptual y contextual sigue una fase de metodología aplicada, que supone el desarrollo del dispositivo Contra como tal, con todas las tentativas técnicas y procesos experimentales que ello comporta. Cabe señalar que durante el desarrollo teórico, pero también dentro de esta fase aplicada, se intercalan casos y prácticas artísticas afines al proyecto, fundamentales para una mejor comprensión del tema y de los elementos simbólicos empleados en la propuesta artística.

2. Una aproximación al poder: de Absolutismo y Liberalismo

¿Qué es el poder? Más allá de su epistemología, que proviene del infinitivo latino possum-potes-potu-posse, capacidad o fuerza para realizar u obtener algo, aún no se ha logrado llegar a un consenso teórico respecto al significado exacto. Por este motivo haremos un análisis esquemático de cómo la aparición del Estado Absolutista implica de un modo inmanente los mecanismos de control en los que se ha evolucionado hasta las Democracias Liberales. Debido a la complejidad del concepto deberemos revisarlo desde diferentes perspectivas, desde lo que podríamos considerar los tres pilares del poder político: Thomas Hobbes, John Locke y Jean-Jacques Rousseau. De este modo anclaremos nuestra historia del poder en la Modernidad, punto del que queremos partir en esta investigación.

Tal y como entendemos actualmente el poder, éste se define como una relación de fuerzas contrapuestas, una especie de lucha antagónica entre los que toman un partido u otro en política, religión, sociedad, etc., aunque veremos que es algo más complejo por la diversidad de lecturas que se han hecho.

Hobbes resuelve el poder en su obra Leviatán como los “medios presentes para obtener algún futuro y aparente bien” (Hobbes 1968, 150) pudiendo ser estos naturales o instrumentales. Su idea del poder natural se basa en las cualidades inherentes a los individuos (fuerza, elocuencia, belleza, etc.), mientras que el poder instrumental es visto como un medio que sirve a los individuos “para obtener más”, respaldando esta teoría a partir de las condiciones naturales del hombre y su suerte. Esto implica que el hombre se mueve por cuestiones meramente impulsivas de sus deseos, como un ser desconfiado que ve peligrar sus intereses por los intereses del otro. En esta situación de temor, el hombre promueve un estado de guerra continuo que Hobbes cree legítimo:

> “Dada esta situación de desconfianza mutua, ningún procedimiento tan razonable existe para que un hombre se proteja a sí mismo como la anticipación, es decir, el dominar por medio de la fuerza o por la astucia a todos los hombres que pueda, durante el tiempo preciso, hasta que ningún otro poder sea capaz de amenazarle. Esto no es otra cosa sino lo que requiere su propia conservación, y es generalmente permitido." (Hobbes s.f, 96)

Hobbes sentencia que el uso de un poder coercitivo, es decir, el uso de la fuerza es un mecanismo para la creación del Estado ya que implica inevitablemente la creación de un contrato social. Esto conlleva una especie de auto-restricción que los hombres se imponen y que sirve como garantía para su propia seguridad y supervivencia, ayudándoles a alcanzar una armonía social. Para lograr dicho fin, los individuos renuncian al ejercicio de sus derechos y libertades naturales, pues, de no ser por esto, Hobbes afirma que todo dependería de la utilización de la fuerza para protegernos individualmente de otros hombres. Así, a través de la necesidad y el miedo, llegamos a la realización de los pactos de poderes para la organización de la vida común, que protegen a todo el que se someta y aseguran su libertad:

> "El mayor de los poderes humanos es el que se integra con el poder de varios hombres unidos por el consentimiento en una persona natural o civil: tal es el poder de un Estado" (Hobbes s.f , 65)

En el desarrollo de este mismo concepto de Estado, pero abandonando la defensa del absolutismo de Hobbes, debemos mencionar a Locke, ya que resulta imprescindible para poder concebir la situación actual y el concepto de democracia liberal. Ambos justifican el origen del poder mediante la creación del contrato social: comparten las mismas categorías del individuo libre, racional e igual en el estado de naturaleza y defienden el pacto como fundamento político que origina el nacimiento de una sociedad mediante la conveniencia de mantener una estabilidad ante una situación de poderes naturales e individuales que pongan en peligro el bien común de una sociedad civil. En este sentido, Locke sostiene que,

> "la falta de un juez común que posea autoridad pone a todos los hombres en un estado de naturaleza; la fuerza que se ejerce sin derecho y que atenta contra la persona de un individuo produce un estado de guerra, tanto en los lugares en los que hay un juez común, como en los que no lo hay". (Locke 2005, 34)

Llegado este punto, Locke y Hobbes describen que, ante la situación de inseguridad del estado, los individuos renuncian a sus libertades de modo irreversible ante la figura soberana. Esto demuestra un acercamiento a las filosofías políticas liberales, las cuales nos muestran que ante cualquier atentado que pueda producirse contra el Estado, podremos ver cómo van siendo eliminados los derechos fundamentales de los individuos. En

Fig. 1 Imagen tomada en zona no autorizada del Polígono da Grela. A Crouña. 2010

resumen, se trata de una representación cuantitativa del poder mediante el contrato social, de la cual se puede desprender una analogía con la actualidad.

Para ejemplificar la consideración actual del Liberalismo hacia la vigilancia, veamos el punto de inflexión que marcaron los atentados del 11 de septiembre de 2001 en EE.UU. A un mes escaso de que se hubiesen producido, tanto la Cámara como el Senado estadounidense sancionaban la ley federal denominada *USA Patriot Act*, un acrónimo de Uniting and *Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act*. Esta ley, que sigue vigente todavía con escasos cambios, tuvo y sigue teniendo el objetivo de ampliar la capacidad de control del Estado con el fin de combatir el terrorismo, dotando a las agencias de seguridad estadounidenses de más potestad sobre la vigilancia y el control social, endureciendo al mismo tiempo las penas por delitos sospechosos de relación con el terrorismo. Recordemos aquí el caso, en pleno apogeo de esta ley, de la detención en 2004 de los bioartistas miembros del CAE (Critical Art Ensemble) Steve Kurtz, profesor de arte en la Universidad de Buffalo, y Robert Ferrell, profesor de genética en la universidad de Pittsburgh, por un supuesto delito de bioterrorismo a causa del material documental de sus proyectos *GenTerra* y *Free Range Grains* sobre investigación biotecnológica.

Como hemos dicho, esta ley ha sufrido algunos cambios, manteniéndose hasta el 31 de mayo 2015 vigente y siendo reemplazada el 2 de junio de ese año por la *USA Freedom Act*, que revoca a la NSA la potestad para el almacenamiento de datos de estadounidenses, si bien se extiende a la jurisdicción internacional. El caso *USA Patriot Act* hace patentes las teorías liberales de Locke y Hobbes que siguen vigentes en la actualidad, porque el régimen tecnológico al que nos hemos sometido en pro de un bien mayor, de una seguridad y de una estabilidad colectivas llevan aparejada la negación de nuestra propia vida.

En el polo opuesto a la teoría liberal de Locke y Hobbes, en la que como hemos visto *el hombre es malo por naturaleza*, se sitúa Rousseau: su visión de la condición natural implica extraer lo mejor de la persona, dándole libertad al niño para desarrollar sus intereses y talentos de forma individual y alejando de él las imposiciones y disciplinas propias de los adultos. Donde más claramente se aprecia su oposición a los filósofos liberales es

en su obra *El contrato social*, donde expone que la fuerza no hace el derecho y que la alienación de la libertad individual y colectiva a un poder hegemónico que se articula verticalmente no es legítima, cuestión que, para Hobbes, sí lo es. En palabras de Rousseau:

> "Renunciar a la libertad es renunciar a la calidad de hombre, a los derechos de la humanidad y a sus mismos deberes. No hay compensación posible para el que renuncia a todo. Semejante renuncia es incompatible con la naturaleza del hombre; despojarse de la libertad equivale a despojarse del ser moral. Por último, es una convención vana y contradictoria estipular, de una parte, una autoridad absoluta, y por la otra, una obediencia sin límites." (Rousseau s.f, 11-12)

La libertad e igualdad del individuo quedan inscritos desde que nace y, al contrario que Hobbes, para Rousseau la renuncia a esta libertad supone la renuncia a la condición de ser humano. Nada más aplicable al momento actual, donde la renuncia a nuestra libertad se manifiesta en la dócil conversión a simples datos digitalizados que se mueven según la necesidad del Estado.

Para evitar esta situación en la que el poder es delegado en la cabeza de un eje vertical, Rousseau habla sobre la necesidad de las pequeñas *agrupaciones sociales*, una situación horizontal que en su dimensión más amplia evoca la idea de Ciudad-Estado. Rousseau asume que el único modo de mantener la libertad individual es que el pueblo se gobierne a sí mismo y mantenga el control sobre los pactos del contrato social. Para Hobbes esto es algo impensable; según él es preferible cierta tiranía soberana y doblegar la voluntad a un solo órgano, porque producirá menos problemas que la vuelta al estado *natural* y a una eventual lucha de todos contra todos por el poder. Según él:

> "Es contrario a la razón alcanzar la soberanía por la rebelión: porque a pesar de que se alcanzara, es manifiesto que, conforme a la razón, no puede esperarse que sea así, sino antes al contrario; y porque al ganarla en esa forma, se enseña a otros a hacer lo propio. Por consiguiente, la justicia, es decir, la observancia del pacto, es una regla de razón en virtud de la cual se nos prohíbe hacer cualquiera cosa susceptible de destruir nuestra vida." (Hobbes s.f, 116)

En la práctica artística, un buen ejemplo de esto podría ser la acción de la artista Tania Bruguera en la *Tate Modern* londinense, *Tatlin's Whisper #5* (2008).

Fig. 2 Tania Bruguera. Tatlin's Whisper #*5*. 2008

En cierto modo, esta acción plasma a las claras el punto de vista de Hobbes: los visitantes del museo discurren por él de un modo caótico, no hay un orden que regule la utilización del espacio, hasta que irrumpen dos policías montados a caballo y comienzan a pautar las acciones y gestionar los movimientos. Los visitantes, a pesar de tener la libertad de *poder hacer*, ya que se encuentran en el marco de una institución cultural, y a pesar de saber que posiblemente se trate de una performance de la artista, son presa del desconcierto y posiblemente por el temor a ser reprendidos permiten que su libertad sea coartada. En palabras de Byung-Chun Han:

> "El deber tiene un límite.El poder hacer por el contrario, no tiene ninguno. Es por ello por lo que la coacción que proviene del *poder hacer* es ilimitada" (Han 2014, 12)

En definitiva, el sistema liberal en el que nos situamos parece haberse apropiado de ambas teorías, manteniendo un eje vertical de sumisión a un poder soberano pero también una aparentemente intocable libertad individual. El entramado tecnológico evidencia la convivencia de ambos extremos, puesto que, aunque en teoría potencia la libertad de los individuos, no es más que uno de los sistemas que el poder ha instaurado para su ejercicio efectivo. Para Hobbes y Locke todo debe estar sometido por el bien, pero ¿quién es ahora el órgano soberano? Ya no queda clara la raíz del poder, pues actualmente

el entramado de las instituciones funciona en la misma medida que las necesidades de las grandes industrias, aunque sobre ella no recae el peso político del Estado sino a la inversa. A esto nos referimos cuando decimos que hemos negado nuestra vida, delegando todo el bien estar y privacidad en una especie de hegemonía invisible que dicta el dónde y el cuándo.

Retomaremos a Hobbes brevemente para recordar que aquello que plantea es que la sociedad se autoimpone restricciones para alcanzar una armonía social. Esta sociedad que se organiza mediante la auto imposición se rige en un orden que se basa en un estado de vigilancia, que mantiene a los individuos en una observación perpetua.

3. El dispositivo

Reflexionar brevemente sobre la noción de dispositivo servirá para estimar su evolución física hacia la invisibilidad de los nuevos sistemas de control, es decir, los actuales dispositivos que usamos diariamente, y también hacia el biodispositivo, que analizaremos a partir de la acción *Time Capsule* de Eduardo Kac y de sus *contra-dispositivos* para promover la inmunidad de los individuos. En palabras de Giorgio Agamben,

> "Llamaré dispositivo literalmente a cualquier cosa que de algún modo tenga la capacidad de capturar, orientar, determinar, interceptar, modelar, controlar y asegurar los gestos, las conductas, las opiniones y los discursos de los seres vivos. Por lo tanto, no solo las prisiones […] sino también la pluma, la escritura, la literatura, la filosofía, la agricultura, el cigarrillo, la navegación, los ordenadores, los teléfonos móviles." (Agamben 2015, 23)

En las sociedades contemporáneas, esa "capacidad de capturar, orientar, determinar, interceptar, modelar, controlar y asegurar los gestos, las conductas, las opiniones y los discursos" está ligadas a todo tipo de dispositivos y pequeños gadgets que podemos ver habitualmente en manos de cualquier ciudadano y que, más allá de su funcionalidad aparente, tienen la finalidad de recopilar información camuflándose bajo la arquitectura opaca de las burocracias digitales. Estas estructuras efectúan un recuento exhaustivo de las actividades personales al tiempo que facilitan su constante localización mediante tarjetas de crédito, teléfonos móviles, etc. (Bauman y Lyon 2013). Esto evidencia lo señalado anteriormente acerca de que el poder ya no es estrictamente coercitivo, ya no se basa solo en la fuerza animal de un cuerpo sobre otro, sino que precisamente potencia la subjetividad para conseguir un sometimiento efectivo del individuo. Uno de los dispositivos más abundantes en nuestro entorno inmediato, el RFID, es buena muestra de ello:

> "desde el ubicuo código de barras que identifica varias clases de productos como del mismo tipo o procedentes de la misma planta, avanzamos hacia los chips de identificación por radiofrecuencia (RFID), que ofrecen identificadores únicos para cada producto individual. Pero no sólo se usan con los productos. Los RFID también se usan en los pasaportes, y en la ropa, y los datos que producen pueden ser conectados sin dificultad con el titular del pasaporte o el que lleva esa prenda." (Bauman y Lyon. 2013. 17)

3.1. De lo material a lo invisible

En el origen remoto de estos dispositivos invisibles de control estaba el alambre de espino, cuyo único propósito era trazar y separar el espacio. Oliver Razac, en *Historia política del alambre de espino*, establece su génesis en el contexto norteamericano, donde este dispositivo jugaba un papel de gran relevancia para establecer la prohibición de paso y la reclusión del ganado, es decir, para doblegar a cualquier animal o sujeto al disuadirlo de un acercamiento físico directo.

La rápida expansión de este dispositivo se vio favorecida por la simplicidad, pero también por su ductilidad y adaptabilidad, es decir, por el hecho de establecer un control espacial de modo orgánico. Con el alambra de espino el confinamiento deja de ser rígido como los muros, eliminando lo superficial, lo sólido, vaciando lo opaco de la fortificación y dejando a la vista únicamente el esqueleto metálico del dispositivo. Esto permite acotar rápidamente los espacios, imponiendo su poder simbólico en la psique de quienes se sitúan a ambos lados de la frontera:

> "el componente dinámico es la capacidad de la cerca para producir una diferencia en el espacio de forma efectiva, es decir, su poder de acción para repeler a los intrusos. Por lo tanto, una cerca es una marca y una acción. No obstante, la problemática general que llevó a la invención del alambre de espino fue el intento de mejorar la relación entre el elemento material de la marca y el elemento eficaz de la acción, la menor marca para la máxima acción" (Razac 2015, 90-91)

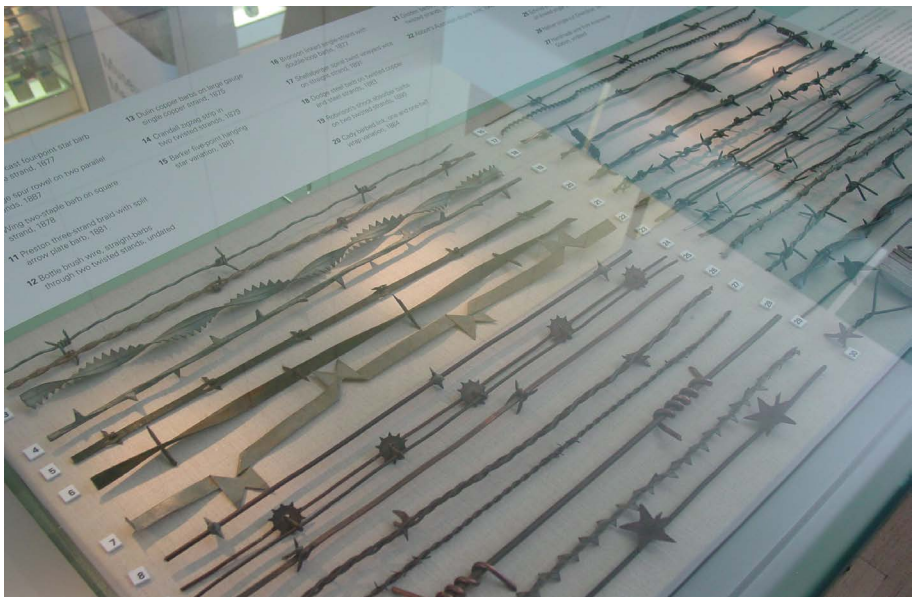


Fig. 3 Catalogación historica sobre el alambre de espino. Melbourne Museum

Esta observación desvela cómo han evolucionado los dispositivos de control, pasando de un sistema físico a un sistema casi invisible que logra ser incluso más eficaz en la organización y el control del espacio al eliminar cualquier ostentación. Este rasgo se ha estilizado al extremo en la actualidad, ya que se evita la coerción física en beneficio de un ejercicio virtual del poder: ya no son necesarios los muros físicos, ahora los límites se crean a partir de algo inmaterial como la luz, las ondas invisibles, las vibraciones (Razac 2015, 30). A esto podríamos añadir todos los sistemas de recopilación y bases de datos que analizan todos nuestros movimientos geográficos, contadores de scrolling y touchs de los dispositivos, que analizan nuestros intereses con el objetivo de optimizar, gestionar y articular el tiempo de nuestras decisiones. En opinión de Razac:

> "No hay que pensar, sin embargo, que el proceso de virtualización signifique la desaparición de las separaciones tradicionales, del mismo modo que la biopolítica no ha desplazado simplemente la soberanía. Tampoco plantea una oposición, sino más bien la creación de un continuo que va de la muralla más maciza a la delimitación más etérea." (Razac 2015, 152)

No necesitamos hacer mucho trabajo de campo para certificar la existencia de esta combinación de dispositivos. En el año 2018, un grupo ciudadano perteneciente a la empresa privada *American Border Patrol*, presidida por Glenn Spencer, uno de los activistas políticos estadounidenses más activos contra la inmigración ilegal en las fronteras, creó el *SEIDARM-MAUI*, un dispositivo basado en sensores sísmicos desarrollado con sensores de sonido y movimiento que se colocan en lugares estratégicos de la frontera entre México y Arizona. Estos sensores no son nuevos en esta práctica, pero la diferencia es la mejora cuantitativa respecto a su sensibilidad: los utilizados por las patrullas fronterizas alcanzan una distancia de entre 6 y 12 metros, mientras que los de *American Border Patrol* alcanzan unos 122, lo que es enormemente significativo a la hora de actuar contra los migrantes.

Existen cientos de combinaciones semejantes por el mundo. Sin ir más lejos entre España y África, uno de los mejores sistemas antiinmigración del mundo y uno de los mayores despropósitos de la historia, aunque en el caso de la frontera española se trate de una actividad promovida desde el mismo *gobierno*, y en el caso anterior el dispositivo fronterizo venga paradójicamente de la mano de un autodenominado *grupo civil ciudadano*.

> “Es fácil considerar la expansión de la vigilancia como un fenómeno tecnológico o como algo asociado al ‘control social’ o al ‘Gran hermano’. Pero al hacerlo se pone todo el énfasis en las herramientas y en los tiranos, y se ignora el espíritu que mueve a la vigilancia, las ideologías que la promueven, las circunstancias que la hacen posible y la gente normal que la acepta, la cuestiona o que decide que, si no puede negarla, se unirá a ella.” (Bauman 2013, 17)

Fig. 4 Shinseungback Kimyonghun. Aposematic Jacket. 2014

3.2. De lo liso y lo estriado

Gilles Deleuze y Felix Guattari proponen en Mil mesetas un par de conceptos que resultan de gran utilidad para entender el mundo digital, lo que denominaron *espacio liso y espacio estriado*. Estos espacios no deben entenderse como opuestos, sino que se subjetivan continuamente sometiéndose a transformaciones:

> "El espacio liso es un campo sin conductos ni canales. Un campo, un espacio liso heterogéneo, va unido a un tipo muy particular de multiplicidades: las multi-plicidades no métricas, acentradas, rizomáticas, que ocupan el espacio 'sin medirlo' y que sólo se pueden 'explorar caminando sobre ellas'." (Deleuze y Guattari 2004, 376)

En cierto modo podríamos analizar este tipo de espacio como un *panóptico*, dado que el espacio liso-pasivo se vuelve estriado-activo en cada acción a la que se somete al vigilado. Foucault proclama que la fuerza del poder coercitivo en las sociedades modernas reside en su capacidad para lograr la *máxima visibilidad* del individuo, y para ello el espacio debe ser liso y estriado al mismo tiempo, ya que los sujetos deben moverse a sus anchas pero sin dejar de ser observados ininterrumpidamente:

> "El que está sometido a un campo de visibilidad, y que lo sabe, reproduce por su cuenta las coacciones del poder, las hace jugar espontáneamente sobre sí mismo, inscribe en sí mismo la relación de poder en la cual juega simultáneamente los dos papeles; se convierte en el principio de su propio sometimiento." (Foucault 187, 2002)

¿Cuál es la estrategia del poder actual a este respecto? Ofrecer un aparentemente liso pero convenientemente estriado en forma de sistemas digitales; el colectivo Tiqqun nos aporta un ejemplo de ello desvelando cómo Google contiene un proyecto implícitamente político en su motor de búsqueda o cómo da a ver determinados lugares y oculta otros. La vieja idea de dominar y consolidar territorios ya no es eficaz, ahora debe proyectarse todo en la manera de acceder virtualmente a él:

> "De acuerdo con este razonamiento, ya no se trata de dar forma al espacio […] sino de adaptarse constantemente a los fenómenos (políticos, sociales, naturales) que trabajan ese espacio" (Razac 2015, 156)

3.3. 24/7

La transparencia que se exige a las nuevas sociedades como método de contención o, mejor dicho, como promesa de una sociedad feliz, implica arrebatar la singularidad al individuo y convertirlo en un objeto funcional necesario para el control (Han 2013, 12). Foucault lo define como una trampa de tecnología. ¿Cómo contratacar ese control? Hakim Bey propone la T.A.Z (*Temporary Autnomous Zone*), en la que "el ataque se hace contra estructuras de control, esencialmente contra las ideas; y la defensa es la 'invisibilidad'" (Bey 2014, 95). No debemos malinterpretar esta sentencia de Hakim Bey en el sentido de querer evadirse políticamente de nuestra responsabilidad o encerrarnos en un búnker, sino que como una manera de entender ese lugar opaco en una *red de islas* autónomas, un lugar donde suceden acontecimientos y en el que podremos, a modo de *máquina de guerra nómada*, atacar, huir y reflexionar sobre una sociedad expuesta en exceso. Según esto, es hora de inmunizarse, de cuestionar la estructura teatral en la que estamos sumergidos sin descanso, de atacar de modo no violento el sistema vigente buscando dispositivos y métodos capaces de estriarse sin dejar de ser lisos –justamente como hace el propio poder.

Actualmente tenemos a nuestra libre disposición un amplio surtido de apps, que van desde los geolocalizadores que siguen nuestro rastro de manera continuada a herramientas que rastrean y almacenan nuestra huella digital a nuestro paso por la red, pasando por un aluvión de información personal que se depositará en múltiples servidores de todo el mundo exponiendo nuestra privacidad y convirtiéndonos a nosotros mismos en vigilantes y sujetos observados.

Véase el caso de lo que se denominó en el periódico La Opinión en 2009 como las Ciberpatrullas. Con el argumento de que los ciudadanos pudiesen vigilar y denunciar el tráfico de drogas, se inició una caza de inmigrantes por parte de los usuarios en la red. Un caso semejante se plasma en la obra *The virtual watchers* (2016), de Joana Moll y Cédric Parizot, una obra que pudimos apreciar y probar personalmente en la LABoral Centro de arte y Creación industrial en la exposición Los monstruos de la máquina y a la que se puede seguir accediendo desde la propia web. La interacción de la obra con el usuario se basa en dejarle adentrarse en las conversaciones, bromas y preguntas del grupo Redservants, encargado de vigilar las fronteras de México.

Fig. 5. Imagen modificada del documental Google Secret War

Fig. 6 Joana Moll y Cédric Parizot. The virtual Watchers

Esta situación de hipervisibilidad a la que estamos expuestos se acentúa con la idea de las sociedades hiperconectadas, en la que la población se halla virtual y constantemente conectada gracias a los nuevos sistemas de comunicación, redes sociales, webs, y todo lo que conlleven los dispositivos móviles. Esto nos permite producir en tiempo real información tanto pública como privada de un modo deliberado sobre otros usuarios. De hecho, la relevancia que han adquirido los sistemas abiertos de vigilancia hace evidente el alcance de los nuevos mecanismos de vigilancia colectiva, donde el control centralizado sobre los comportamientos ha ido dejando paso a formas de supervisión multitudinaria. En palabras de Bauman:

> "La existencia de las redes sociales depende de su capacidad para observar el comportamiento de los usuarios y vender esos datos a otros. Las posibilidades de resistencia en una red social son atractivas y en algunos casos pueden se eficaces, pero también tienen límites: en primer lugar debido a la falta de recursos para establecer relaciones personales en un mundo líquido, y en segundo lugar por el poder de la vigilancia dentro de esos medios de comunicación sociales, que es endémico y muy poderoso." (Bauman y Lyon 2013, 12)

Este hecho produce una grave contrariedad, ya que Internet era la herramienta que en teoría democratizaría las comunicaciones, el libre flujo de ideas, las opiniones y el conocimiento. Un canal que nos podía servir para burlar el totalitarismo de los Estados, abriendo espacios de igualdad, pero que en realidad ha contribuido más al refinamiento de las sociedades controladas. Recordemos en este sentido uno de los hechos que acontecieron en el momento álgido de la Primavera Árabe en Egipto, en 2011: el régimen de Hosni Mubarak, ante las movilizaciones que se

promovieron desde las redes sociales, decidió cortar todas las conexiones del país (Twitter, Facebook, telefonía móvil, etc.). Este ha sido el apagón a mayor escala en la historia de las comunicaciones, sin olvidar que hubo otros casos como Birmania en (2007) o Irán (2009).

Hay que tener claro que las redes sociales, Internet, etc, no son necesariamente herramientas de democratización, sino que se trata de sistemas que no practican una dicotomía a la hora de diferenciar por quién son empleadas. Su crecimiento rizomático ha contribuido al desarrollo de un régimen de control social difuso y difícil de localizar. Como dijo el periodista Andrew Sullivan parafraseando el himno "The revolution Will Not Be televised" de Gil Scott-Heron (1970), "The Revolution Will Be Twittered".

Debemos analizar todo este engranaje que, igual que sirve para perseguir y castigar a cualquiera que se considere opositor al grupo de poder, también sirve para dar rienda suelta a la libertad de expresión: la paradoja de *Internet* es que la utilizan desde los revolucionarios hasta el propio Estado y sus autoridades. Como bien señalaba Niklas Luhmann, "el poder se incrementa con las libertades de ambas partes: por ejemplo, crece en una sociedad en la medida en que ella genera alternativas" (Luhmann 1977, 9).

Fig. 7 Colectivo WIDEPHOTO. Botón para apagar internet

El colectivo WIDEPHOTO, desde un punto situado entre la sátira y la crítica, refiere esta situación de superioridad tecnológica por parte del Estado con una acción donde invitaba a la gente a usar

la máscara de uno de los líderes mundiales que han censurado Internet; en el contexto del *Mercado de pulgas Yami-Ichi* como parte del festival *Influencers* en Barcelona, a los participantes se les daba el poder de presionar el botón rojo y apagar Internet.

El caso de PRISM, que salió a la luz en 2013, permitió constatar la vulnerabilidad de los usuarios ante el espionaje y la venta de datos personales. PRISM es un programa que permite acceder a la información que almacenan los servidores de varias multinacionales como Facebook, YouTube, Google, etc, sobre todo historiales de búsqueda de los usuarios, correo electrónico, transferencia de archivos, datos de geolocalización y live chats. Sin embargo, este suceso no aislado pasó desapercibido o se olvidó con tanta rapidez como otros. Véase el caso de Edward Snowden, quien filtró documentos de la CIA; o el de Julian Assange, creador de WikiLeaks, portal de difusión de información comprometida con casos de altos cargos de poder; o el de Chelsea Manning, la exsoldado analista de inteligencia del ejército de Estados Unidos que filtró a WikiLeaks documentos clasificados de la guerra de Afganistán, conocidos como los *Afghan War Diary*, o el vídeo conocido como *Collateral Murder*. Estas situaciones de exclusión, castigo y olvido se dan por una cuestión simple de crecimiento geométrico, en el que el poder crece proporcionalmente en función del incremento de las alternativas de resistencia, como señalaba Luhmann. Aunque *Internet* mantiene su espíritu en cierto aspecto democrático, no deja de ser por este mismo motivo un recurso en manos de las élites: a pesar de su capacidad para desvelar y argumentar, la autoridad del Estado tiene a su disposición el botón de apagado.

Fig. 8 Logo del programa PRISM, diseñado a partir de la adaptación de manera ilegal de una fotografía de Adam Hard-Davis

Analizar esta situación desde casos concretos es fundamental para comprender las relaciones entre los individuos y el Estado en la actualidad y para visualizar fenómenos de autoridad, ya que en ellos se establecen roles en los que se constituye un poder de mando y un poder de obediencia que a menudo parece difuso. En palabras de Foucault, estos procedimientos:

> "determinan la conducta de los individuos, los someten a cierto tipo de fines o dominación y consisten en una objetivación del sujeto […] Estos tipos de tecnología casi nunca funcionan de forma separada, aunque cada una de ellas esté asociada a algún tipo particular de dominación. Cada una implica ciertas formas de aprendizaje y modificación de los individuos, en la adquisición de ciertas habilidades y actitudes." (Foucault 1990, 45)

Debemos entender que a mayor crecimiento de dispositivos es lógico que proliferen los procesos de subjetivación, y más en una época como esta, donde cada día surgen actualizaciones de dispositivos y se generan otros nuevos. En ningún momento se ha abandonado la antigua praxis disciplinaria, solo que ahora el dispositivo ya no parte simplemente del intermediario, sino que ha mutado en una interfaz que modula el cuerpo social. Volvemos así al concepto de panóptico, pero desde una nueva perspectiva: la dinámica básica es observar a los individuos supervisando y determinando sus comportamientos privados de manera constante. Siendo así, ¿qué diferencia entonces la mirada centralizada de las redes sociales, que como hemos dicho no solo sirven para la congregación y reivindicación de derechos, sino que como un dispositivo de regulación global? Véanse Instagram o Facebook, donde podemos acceder a un amplio catalogo de individuos que al mismo tiempo que son estandarizados mediante poses, caracteres, situaciones, etc., estandarizan al observador. El dispositivo portátil gobierna la vida social por completo:

> "Probablemente no sería errado definir la fase extrema del desarrollo capitalista que estamos viviendo como una gigantesca acumulación y proliferación de dispositivos. Es cierto que hubo dispositivos desde que apareció el homo sapiens, pero parecería que hoy no hay un solo instante en la vida de los individuos que no esté modelado, contaminado o controlado por algún dispositivo […] Aquel que se deja capturar en el dispositivo 'teléfono móvil', cualquiera que sea la intensidad del deseo que lo ha movilizado, no adquiere por ello una nueva subjetividad, sino sólo un número a través del cual eventualmente puede ser controlado." (Agamben 2015, 25-31)

Demos ahora un paso más allá y veamos un ejemplo de dispositivo que está en proceso de creación, la *Smart city* o *ciudad inteligente,* que dispondrá tanto de apps como dispositivos físicos instalados en el espacio para el análisis de los movimientos de las masas y decidir en qué lugar deben estar, tanto para situarse en estos espacios como para la elección de lugares a los que deben asistir. Aunque esto pueda parecer inocente, en realidad es unos de los sistemas de control más efectivos, ya que replantea la idea de Panóptico creando nuevas estrategias en el espacio abierto.

Estos esquemas de movilidad se desarrollan en una escala de control semejante a la mecánica de movimientos, gestos y agilidad del cuerpo que describe Foucault: como una coerción constante que permite el control disciplinario sobre las operaciones del

individuo. La acción sobre el cuerpo del individuo no se suprime por completo, es decir, no hay una apropiación de éste, sino que persigue hacerlo útil abandonando el centro de acción sobre lo físico y llevándolo a su psique. El individuo solo es útil por su fuerza de trabajo siempre y cuando a la vez sea productivo y dominable, aplicando sobre él la microfísica de poder político que lo desarticula y lo recompone. Un conjunto de subjetivaciones que dan forma al dispositivo de poder y transmuta al individuo, individualizándolo y desarticulando del colectivo, definiendo el lugar que ocupa cada individuo, atravesándolo para dominarlo y reorganizando lo múltiple, evitando cualquier congregación o formación del colectivo que pueda cuestionar la jerarquía de poder. Como indica Peter Sloterdijk,

> "De ahí que en el seno de la sociedad posmoderna esta masa, que ya no se reúne o congrega ante nada, carezca de la experiencia sensible de un cuerpo o de un espacio propios; ella ha dejador de percibirse como una magnitud capaz de confluir y actuar [...] cargadas de deseo y negatividad pre-política, oscilan en sus espacios propios, mientras, inmóviles ante sus aparatos receptores de programación, consagran individualmente sus fuerzas una y otra vez a la solitaria tentativa de exaltarse" (Sloterdijk 2017, 18)

Planteemos a partir de esto una cuestión: ¿en verdad la relación humano-dispositivo se realiza bidireccionalmente? Nosotros dotamos de identidad a los dispositivos y ellos subjetivan la nuestra, pero quizá estemos solo siendo subjetivados por el dispositivo y no a la inversa, y puede que nuestra capacidad de creación se replantee en una sola dirección, la de las necesidades creadas por el aparato.

Fig. 9 Moby. Fotogram videoclip *Are you lost in the world like me?*. 2016

4. Bio

Esta circunstancia conduce directamente al concepto de biopolítica, acuñado por Foucault y desarrollado por autores como Roberto Esposito o Giorgio Agamben. Todos ellos abordan la gestión de la vida y la muerte, el biopoder y la inmunidad, y aunque trataremos brevemente en sus aportaciones, nos centraremos en la teoría de Esposito por su afinidad a la cibernética y a la gestión de la vida digital en las sociedades del control y muy especialmente por su concepto de *inmunidad*, sobre el cual gravita en buena medida el proyecto CONTRA.

4.1. Biopolítica

En el citado ensayo *Vigilar y Castigar*, Michel Foucault plantea que un dispositivo es cualquier tipo de subjetivación del individuo a través del condicionamiento físico y psicológico. Foucault hace un repaso sobre el cuerpo como máquina desde el siglo XVII, y aunque no existe la intención de realizar aquí un análisis de ello, nos servirá para comprender la idea de biodispositivo con mejor perspectiva.

Foucault alude con el término de biopolítica a un momento histórico concreto en el que la gestión de la vida pasa a ser un monopolio del poder. Durante el siglo XVII la capacidad de administrar la vida y la muerte se caracteriza por una inclinación hacia la segunda –el soberano ejercía el poder sobre el individuo en la medida en que podía decidir matarlo–, pero con la llegada del siglo XIX este derecho se modifica en beneficio del poder de *hacer vivir*: ya no se administra la muerte, sino que se persigue hacer al sujeto más útil y eficiente, es decir, más *vivo*:

> "El derecho de muerte tendió a desplazarse o al menos a apoyarse en las exigencias de un poder que administra la vida, y a conformarse a lo que reclaman dichas exigencias. Esa muerte, que se fundaba en el derecho del soberano a defenderse o a exigir ser defendido, apareció como el simple envés del derecho que posee el cuerpo social de asegurar su vida, mantenerla y desarrollarla." (Foucault 2005. 165)

Deja de tratarse el cuerpo como si fuera indivisible: el control ya no se aplica como disciplina sobre el individuo, sino que se aplica al control del cuerpo social en conjunto ya que este repercute directamente en lo físico individual. En esta administración del *cuerpo social*, la biopolítica pasa a ocuparse de dominar lo

físico con vistas a la mejora de su mecanismo productivo, como evidencian las técnicas empleadas en el ejército, los colegios, las fábricas y los espacios penitenciarios con vistas a la obtención cuerpos dóciles (Foucault 2002, 126), pero también los espacios de entrenamiento que son los gimnasios.

El ejemplo actual más palpable de este hecho, al que todos tenemos acceso tanto siendo socios de un gimnasio como en los video tutoriales en cualquier plataforma de streaming en internet, son las clases monitorizadas, algo de lo que personalmente hemos sido participes y que lleva siempre el termino *BODY* y eventualmente acompañado de otro sustantivo del tipo power, balance, combat, etc. En todas ellas se busca la optimización del cuerpo y los tiempos de eficiencia: como describe Foucault, no se centra en elementos significativos de la conducta o el lenguaje del cuerpo, sino en la economización de los recursos de este, en la eficacia de los movimientos y en su organización interna a la hora de articular el conjunto no solo del intermediario que ejerce como monitor de la clase, sino del poder que ejerce el colectivo, que reacciona de manera unísona al mandato guiado por el ritmo repetitivo de los sonidos y los lemas motivadores. Con este ejemplo tratamos de remarcar que los mecanismos utilizados durante el siglo XVII y XVIII siguen vigentes, pero con un sistema que por un lado se relaciona a la idea de colectivo y por otro a lo aparentemente lúdico.

Hemos visto que para Foucault la vida se incluye en la política únicamente en la modernidad; en cambio, para Agamben el derecho soberano de administrar la vida es propio de la política, centrando la atención en el rol que realiza el Estado como creador del cuerpo biopolítico y su cometido es la regulación de este:

> "Se puede decir, incluso, que la producción de un cuerpo biopolítico es la aportación original del poder soberano. La biopolítica es, en este sentido, tan antigua al menos como la excepción soberana. Al situar la vida biológica en el centro de sus cálculos, el Estado moderno no hace, en consciencia, otra cosa que volver a sacar a la luz el vínculo secreto que un el poder con la nuda vida." (Agamben 1998, 16)

De este modo, mediante la idea de excepción de la política occidental, la soberanía circunscribe la vida en lo jurídico a través de la exclusión, planteando de manera opuesta a Foucault que la biopolítica ha estado siempre incluida dentro del poder soberano. Este mecanismo de exclusión de la vida natural

(*zoe*) que caracteriza la política occidental es en realidad una exclusión inclusiva, *una exceptio* (Agamben 1998, 17) de la *zoe*. Para remarcar que la vida siempre ha pertenecido a la política, Agamben dice que la excepción soberana es "el dispositivo original a través del cual el derecho se refiere a la vida y la incluye dentro de sí por medio de la propia suspensión" (2004, 24).

Según el planteamiento de Agamben, las formas políticas modernas –democracia, representatividad, etc.– no podrían incluir la vida biológica sin el precedente del poder soberano para gestionar la muerte. Hagamos un breve inciso para recordar a Hobbes, para quien la comunidad política solo se puede formar en cuanto se abandona el estado de naturaleza, de guerra continua por la satisfacción de deseos individuales, y se cede la voluntad del sujeto al soberano. Esta comparación demuestra que en todo momento se ha hecho una separación entre lo que se encuentra dentro del orden soberano (sociedad civil o bios) y lo que se excluye fuera de esta (estado de naturaleza o zoé).

4.2. Biodispositivo

La reflexión sobre el biodispositivo se suscita a raíz de la obra de Eduardo Kac *Time Capsule*, quien se injerta un microchip con sus datos personales y retransmite la acción en directo mediante televisión e internet, dando lugar a un post-panóptico interno e invisible que monitoriza en tiempo real al individuo donde quiera que se encuentre.

Tratadas esquemáticamente las teorías de Foucault y Agamben, la teoría de Roberto Esposito hila con la teoría de Agamben desde el paradigma inmunitario y nos sirve como puente hacia la *Hipótesis cibernética* que plantea Tiqqun (2015). En palabras de Esposito,

> "Sólo si se la vincula conceptualmente con la dinámica inmunitaria de protección negativa de la vida, la biopolítica revela su génesis específicamente moderna. No porque no haya una raíz de ella reconocible también en épocas anteriores, sino porque sólo la modernidad hace de la autoconservación del individuo el presupuesto de las restantes categorías políticas, desde la soberanía hasta la de libertad." (Esposito 2006. 17-18)

En este caso nos centraremos en la relación dialéctica entre comunidad e inmunidad propuesta por el filósofo italiano, que hace de la inmunidad el problema por excelencia de la comunidad.

Esposito argumenta que el poder se adentra en la comunidad para protegerla, por lo que cree necesario someterla a sistemas inmunitarios que resguarden la vida mediante mecanismos de control negativos, los cuales al mismo tiempo le negarán su libertad hasta el punto de que convertir la política de vida en política de muerte:

> "La inmunización es una protección negativa de la vida. Ella salva, asegura, preserva al organismo, individual o colectivo, al cual le es inherente, pero no lo hace de manera inmediata, frontal, sino, por el contrario, sometiéndolo a una condición que a la vez niega, o reduce, su potencia expansiva." (Esposito 2006. 74-75)

Volvemos en este punto al alambre de espino, entendido ahora como un biodispositivo que concede o niega la vida de quien intenta traspasarlo, convirtiéndose en un mecanismo hiperinmunitario, una vacuna para salvaguardar el cuerpo de sus ciudadanos que finalmente puede plegarse sobre sí misma y volverse en su contra encerrándolo en el espacio:

> "el mal que ataca al cuerpo político -se trate de una invasión extranjera o de un conflicto civil- tiene su matriz patógena fuera de él y se le trasmite por medio de la infiltración de un elemento contagioso no generado por el propio organismo. […] De aquí la necesidad, cada vez más enfatizada, de barreras, protecciones y aparatos inmunitarios tendentes a reducir, si no a eliminar, la porosidad de las fronteras externas contra los gérmenes tóxicos contaminantes" (Esposito 2005. 174-175)

El mal tiene así un rasgo positivo, porque "la enfermedad refuerza por contraste, o inclusive crea, los mecanismos autodefensivos del organismo enfermo" (Esposito 2005. 176). El modo crítico más poderoso para ello es utilizar el propio sistema para anularlo, volver poroso el terreno, hacerlo transparente y facilitar la fracturar de sus divisiones: "nada, comparado con un mal dominado y vuelto contra sí mismo, refuerza más el cuerpo político que lo alberga" (Esposito 2005, 176). Respecto a la idea de usar el propio sistema para combatir el sistema, recordemos el caso de la Primavera Árabe y el uso de las redes sociales para congregar el cuerpo social. Como observa el llamado Comité Invisible,

> "Queda cada vez más claro que Facebook no es tanto el modelo de una nueva forma de gobierno, sino su realidad ya operativa. Sin embargo, el hecho de que algunos revolucionarios hayan empleado esa herramienta

(y aún lo hagan) para vincularse masivamente en las calles, solamente demuestra que es posible, en ciertos casos, usar Facebook en contra de sí mismo: en contra de su función esencial, que consiste en hacer de policías." (Comité Invisible 2015, 335)

A partir de los conceptos de inmunidad y biodispositivo, remarcamos el carácter de CONTRA en el sentido de un mecanismo dotado de capacidad para inmunizar, pues "introduce en el interior del organismo a proteger un agente patógeno despotenciado que activa la reacción inmunitaria y salvaguarda la seguridad del inmunizado, pero al precio de desnaturalizar la respuesta vital" (Bazzicalupo 2016, 163).

Esta capacidad se ve reflejada en la sentencia de Deleuze y Guattari, en la que exponen:

"Si las máquinas motrices han constituido la segunda edad de la máquina técnica, las máquinas de la cibernética y de la informática forman una tercera edad que recompone un régimen de esclavitud generalizada: —sistemas hombres-máquinas, reversibles y recurrentes, sustituyen a las antiguas relaciones de sujeción no reversibles y no recurrentes entre los dos elementos; la relación del hombre y de la máquina se hace en términos de de uso o de acción, sino de mutua comunicación interna" (Deleuze, y Guattari 2004, 463)

5. Práctica artística

En este apartado desarrollaremos el trabajo práctico, que se ha realizado dentro del marco de esta investigación en lenguajes audiovisuales, cultura social, interacción y comportamientos, y adscrito a su vez a las subcategorías de resistencia, nuevos medios y diseños de interfaz. Desarrollaremos antes que nada los estados previos al proyecto inspirándonos en los textos The *Critical Engineering Manifesto* y *Desobediencia civil electrónica.*

Fig. 10 Miguel Sislian Suez. CONTRA. 2018

5.1. Planteamiento

Desde que comencé mis estudios en arte en el instituto, y posteriormente especializándome en un módulo técnico superior de fotografía artística y en un grado en Bellas Artes, he trabajado en la representación pictórica de la identidad. Igualmente he trabajado en el campo audiovisual esta temática relacionada a la construcción del yo basada en los recuerdos reconstruidos y también en la memoria sonora y la creación de ficciones mediante objetos sonoros. Siempre he tenido interés por los sistemas digitales y las comunicaciones, pero no fijé este interés hasta comenzar el Máster de Artes Visuales y Multimedia, que marcó la dirección hacia este proyecto.

Contra: Interfaces para la resistencia surgió por la necesidad de crear un dispositivo de insurgencia que reflexionase sobre la necesidad de la inmunización del individuo. Durante el teórico hemos trabajado los conceptos de poder, control y vigilancia que se han establecido llevándolos a la era digital, haciendo patente nuestra dependencia a los dispositivos, los cuales marcan cada acción de nuestra vida. Lo que se plantea en este proyecto, es una alternativa de pequeña resistencia convirtiéndonos en un sistema invasor en tiempos de la vigilancia digital.

5.2. T.U.I

Las TUI o *tangible user interface* por sus siglas, son interfaces con las que el usuario puede interactuar con información digital a través de un elemento físico. El propósito de estas interfaces es potenciar la colaboración, el aprendizaje mediante la creación y el diseño al dar una forma tangible a información digital.

5.2.1. Materiales

Durante la fase de creación de la interfaz CONTRA, se investigó sobre materiales conductivos que nos sirviesen para su creación. Textiles como el fabricado por la empresa NASAFES, facilitado por un compañero del máster, o las propias mantas isotérmicas, que están compuesta por una fina película de plástico aluminizada por las dos caras, con la característica de ser altamente conductivas. Esto nos llevó a las primeras experimentaciones en el uso de materiales que ofrecieran la posibilidad de ser programados con Arduino para su implementación e interacción mediante capacitivos en proyectos de textiles inteligentes.

Fig. 11Tejido conductivo NASAFES

Fig. 12 Manta Isotérmica

Los dos materiales tienen la característica de tener una buena conductividad, especialmente en el caso del tejido de NASAFES, que por su composición de polyester y níquel es mejor conductor y al mismo tiempo bloquea cualquier onda electromagnética. La manta isotérmica goza de aislamiento térmico, como su nombre indica, por lo que evita el reconocimiento mediante cámaras térmicas. Precisamente en el manual *Dron Survival Guide* se ofrece una explicación para evitar ser localizado mediante sistemas de comunicación o visores térmicos montados en los drones gracias a las mantas isotérmicas y sistemas de jamming.

Esta fue una fase compleja debido a cuestiones de electrónica, ya que a pesar de lograr el objetivo hubo muchos inconvenientes en el apartado de circuitería a causa de la inexperiencia personal a la hora de crear placas: desde circuitos que producían mucha resistencia por el tipo de strips de las placas, componentes difíciles de obtener en tiendas habituales, a quemados y placas muy inestables a la hora de funcionar, todo fueron contratiempos.

5.2.2. Prototipos

En los primeros estadios del proyecto se perseguía trabajar con el sonido, más concretamente con ondas ultrasónicas e infrasónicas, concertinas y mantas isotérmicas, pero pronto se comenzó a crear prototipos basados en los materiales descritos.

Prototipo fase 1

El primero prototipo se planteó como un dispositivo de geolocalización espacial, que funcionaba mediante un *sensor ultrasónico HC-SR04* montado en un servomotor que giraba continuamente en un ángulo en 180 grados de derecha a izquierda y viceversa detectando a los usuarios en el espacio. Ambos sensores fueron programados mediante Ide Arduino.

Para el mapeo de estos datos, mediante Processing se realizó un modelo visual de un sistema simple de radar que se proyectaba en la pared para mostrar el funcionamiento del sensor, que mediante líneas de diferentes distancias marcaba los obstáculos. El output de Processing se comunicaba mediante Pure Data, que al recibir los datos del sensor generaba una onda *infrasónica* digital a 20Hz. El resultado de estar expuesto a esta frecuencia de sonido durante un periodo de tiempo prolongado podía producir malestar físico.

Fig. 13 Fase 1. El muro invisible. 2017

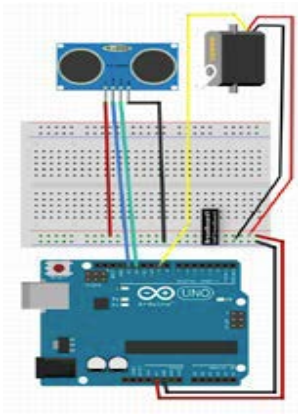


Fig. 14 Fase 1Diagrama conexiones. 2017

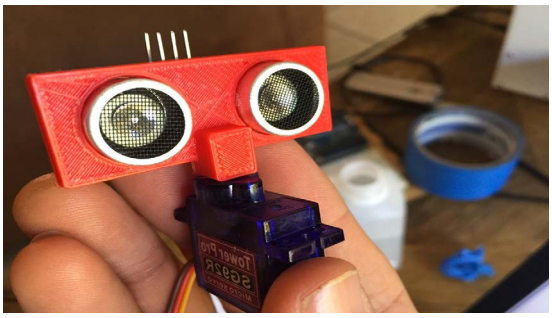


Fig. 15 Sensor de ultrasonido con servomotor. 2017

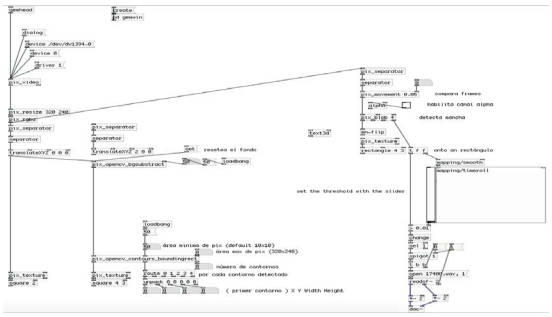


Fig. 16 Programación Pure Data. 2017

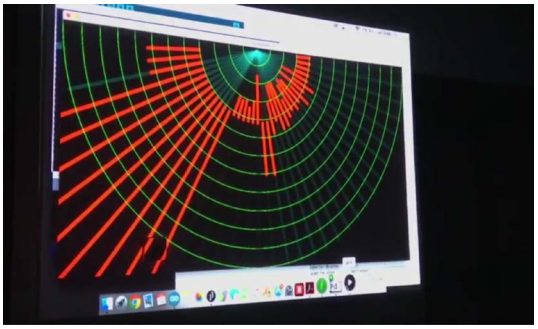


Fig. 17 Visual hecho con Processing. 2017

Prototipo fase 2

En la posterior etapa del proceso creativo, buscamos otros métodos y materiales que pudiesen enriquecer el proyecto a nivel técnico, por lo que comenzamos a trabajar con el sistema de video tracking.

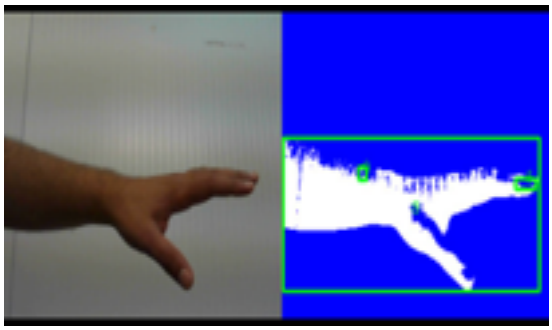


Fig. 18 Captura de la webcam. OpenCV. HardCascade. 2017

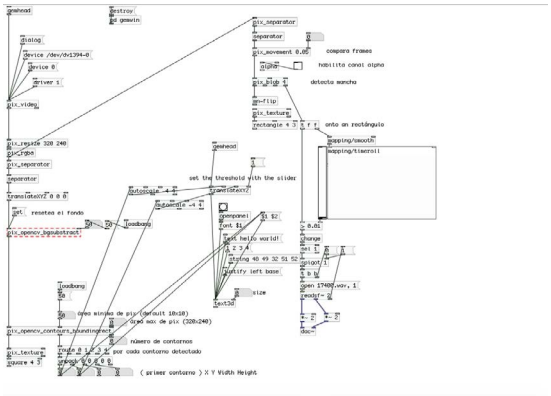


Fig. 19 Programación Pure data. OpenCV. 2018

Para esto usamos una librería de OpenCV (*computer visión*) de Pure Data, que al detectar usuarios emitía un sonido ultrasónico para provocar un estado de incomodidad que obligase al usuario a salir de la sala. Esta frecuencia estaba generada digitalmente en Pure Data al igual que el primer prototipo, usando la misma parte de programación para sonido.

A la vista de la poca efectividad del segundo prototipo, que no llegaba a convencer sobre lo que estábamos investigando, se optó por volver al primer prototipo y se dejó temporalmente la idea de hacer un dispositivo sónico para esta investigación.

Prototipo fase 3. CONTRA

Fig. 20 Primer prototipo digital. CONTRA. 2018

Como se mencionó en los antecedentes del proyecto, se ha pasado por diferentes etapas y prototipos desde la idea inicial del mismo, lo que ha desembocado en la idea del wearable que trataremos como biodispositivo. ¿Por qué se expone éste como biodispositivo? Aunque el término es aplicado generalmente en el campo de la medicina o el *biohacking*, en este caso se ha acuñado a la interfaz *Contra* basándonos en la teoría de Roberto Esposito sobre la inmunidad, y porque su funcionamiento depende del propio cuerpo del usuario.

Durante la fase de rastreo de referentes en arte, se formalizó la intención de lo que se quería representar: una interfaz de carácter crítico de tipo TUI (*Tangible User Interface*) que se presentase como un *wearable*. Durante la fase inicial este pretendía ser una chaqueta al uso hecha a partir de mantas isotérmicas, pero se descartó por la funcionalidad y la rigidez a la que habría que estar sometido para no destruir el material, que en un uso diario se deterioraría con facilidad. Por este motivo se decidió investigar otro tipo de prenda que, además de resistir el uso, tuviese un simbolismo más directo con el concepto de protección. La idea de realizar un *wearable* se vio reforzada a partir de una noticia sobre empresas que aprovechando el estado de inseguridad ciudadana generado por los atentados se han dedicado a vender todo tipo de *wearables*: antibalas, anti-cortes por arma blanca, rastreadoras, etc. Para este proyecto, el *wearable* que más nos interesó fue la *Trailblacer* de la empresa *Bladerunner,* una chaqueta con un GPS integrado para mantener localizado al usuario en todo momento.

La interfaz que finalmente se ha confeccionado se basa en la idea de invisibilidad ante los sistemas de vigilancia digital, idea que obtuvimos de *Dron survival guide* del artista Ruben Pater.

Fig. 21 Ruben Pater. Dron Survival Gudie

Fig. 22 Segundo prototipo digital. CONTRA. 2018

Se trata de una capa de invisibilidad que reproduce la forma de un chubasquero y funciona mediante la programación de un NodeMCU ESP8266 junto a una extensión de circuito jammer que hemos hackeado para que el NodeMCU le envíe datos para la emisión de interferencias de telefonía y localización.

Fig. 23 Bocetos. CONTRA. 2018

5.2.3. Confección del wearable

Se acompañan en este punto imágenes del proceso de confección del wearable que intentan describirlo visualmente en todos sus extremos: patrones, sistema de medidas y registro fotográfico del proceso

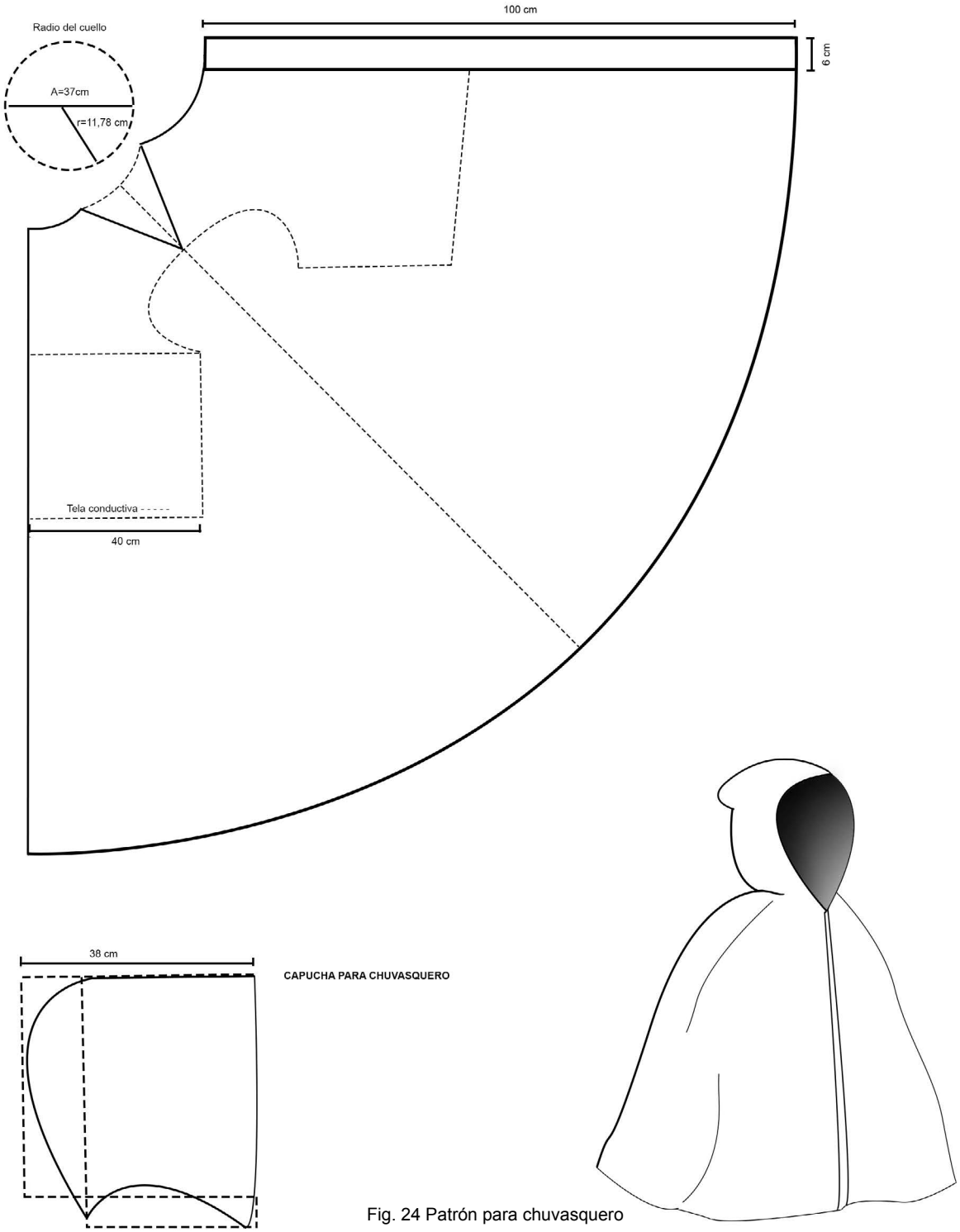


Fig. 24 Patrón para chuvasquero

Para la realización del patrón de la capa, buscamos en internet un modelo de patronaje y lo adaptamos a nuestras necesidades. Primeramente, se reforzó la manta isotérmica con tela adhesiva para evitar que el movimiento brusco pudiese dañarla. Posteriormente se realizó el dibujo del patrón usando una tiza y una cuerda a modo de compás, lo cual nos permitió realizar la semicircunferencia del bajo y el largo de la capa, que se recortó dejando dos centímetros para poder hacer el remate sin perder las medidas.

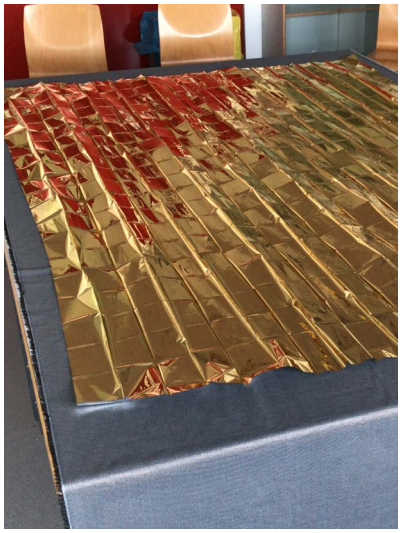


Fig. 25 Corte y confección para capa CONTRA

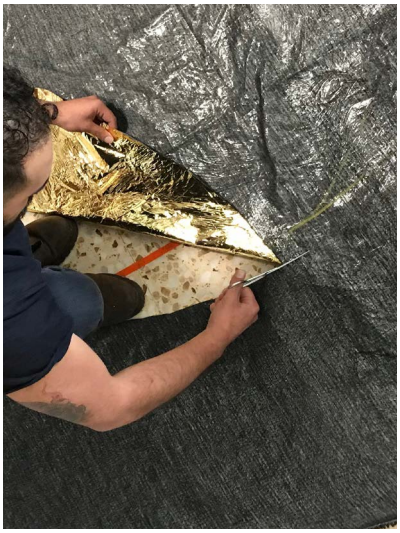


Fig. 26 Corte y confección para capa CONTRA

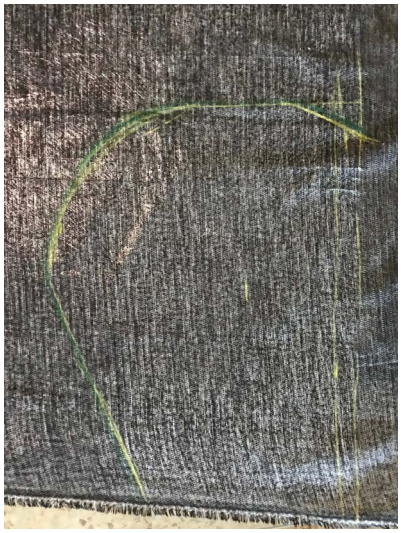


Fig. 27 Corte y confección capucha CONTRA

Fig. 28 Corte y confección capucha CONTRA

Para la capucha se llevó a cabo el mismo proceso que para la capa. Primero se midió la circunferencia de la cabeza y la del cuello para evitar que pudiese quedar pequeña. Posteriormente se dibujó la forma y la caída de la capucha para finalmente recortarla y confeccionarla.

Finalmente se hizo el corte del textil conductivo. Nuevamente hubo que media la circunferencia del cuello para poder hacer el corte a la medida. Finalmente se cortó, y se hizo un remate con hilo conductivo para evitar cualquier interferencia.

Fig. 29 Corte y confección téxtil NASAFES CONTRA

Fig. 30 Corte y confección téxtil NASAFES CONTRA

Fig. 31 Corte y confección final CONTRA

Para la fase de costura a máquina, debido a la falta de experiencia en el campo de la confección y los anteriores intentos frustrados, fuimos asistidos por la artista plástica Dela Delos (Alicia de la Fuente de los Ángeles) que aportó toda su experiencia en este campo ayudándonos a trabajar el delicado material con un acabado profesional.

5.3. Electrónica

Durante esta fase, se ha investigado sobre los dispositivos WiFi e inhibidores móviles, bandas de frecuencias, tipos de antenas, así como la legislación dentro del territorio nacional, para poder desarrollar con éxito este proyecto que ha sido apoyado por personal docente de telecomunicaciones de la Universitat Politècnica de València.

Terminada la fase de búsqueda de dispositivos jammer, la más compleja dada la dificultad en cuanto a la programación y electrónica, nos centramos en los elementos simbólicos del proyecto: el dispositivo para la inmunización. La idea de integrar dispositivos en la interfaz se plantea con la intención de producir una interacción por parte del usuario que genere una relación con el hardware. Esta interacción activa el wearable, produciendo la anulación de redes móvil y wifi que estén presentes en el entorno, ya sea en el contexto del espacio expositivo o fuera de él.

Por la extensión del proceso de instalación del NODEMCU ESP8266 creemos conveniente añadir en este documento solo las modificaciones del código y la programación de otros componentes que no han requerido demasiada extensión en un anexo. No obstante, todo el material estará disponible en el repositorio de GitHub que se proporcionará en el apartado de revisiones web junto con el link de la web *instructables* en la que seguir paso a paso lo básico para la instalación de las librerías para el *Jammer* WiFi.

5.3.1. Dispositivos y funcionamiento

El funcionamiento de circuito está dividido entre dos microcontroladores. Node MCU es una plataforma Open Source que tiene integrado un microchip ESP8266 para comunicaciones WiFi. Para este proyecto ha sido programado a partir de librerías *open source* para que, al ser activado, ejecute una serie de acciones que hemos automatizado para que escanee las redes

cercanas y la MAC de los clientes que posteriormente, desconecta todos los dispositivos mediante un ataque *deauthentication*. Este ataque consiste en hacerse pasar por el punto de acceso y mandar a todos los clientes paquetes de desautentificación.

Este tipo de ataque para entenderlo sin adentrarnos es demasiadas especificaciones, debemos explicar que es el estándar IEEE 802.11. Este es un paquete propio que utiliza el Punto de acceso inalámbrico durante su funcionamiento que le dice al cliente que se desconecte. Lo que se realiza en este proyecto se podría ejemplificar del siguiente modo: cuándo el router tiene el máximo de conexiones de clientes que puede soportar o que se han configurado previamente en dispositivo de conexión, los próximos clientes que intenten conectarse se les envía un paquete deauth para evitar su conexión.

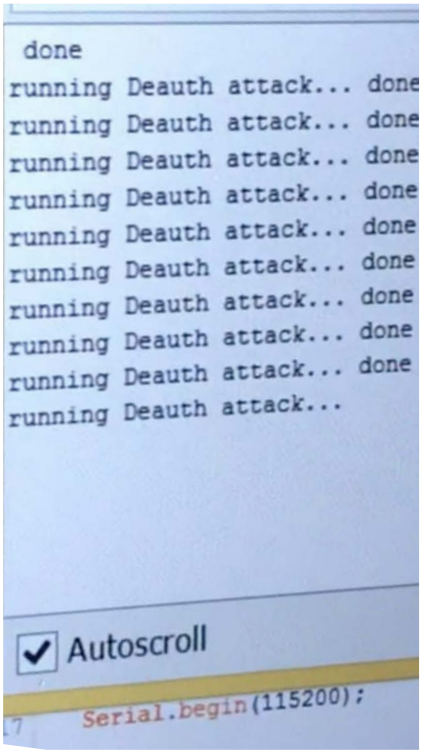


Fig. 32 Datos de ataque de la deconsola Arduino IDE

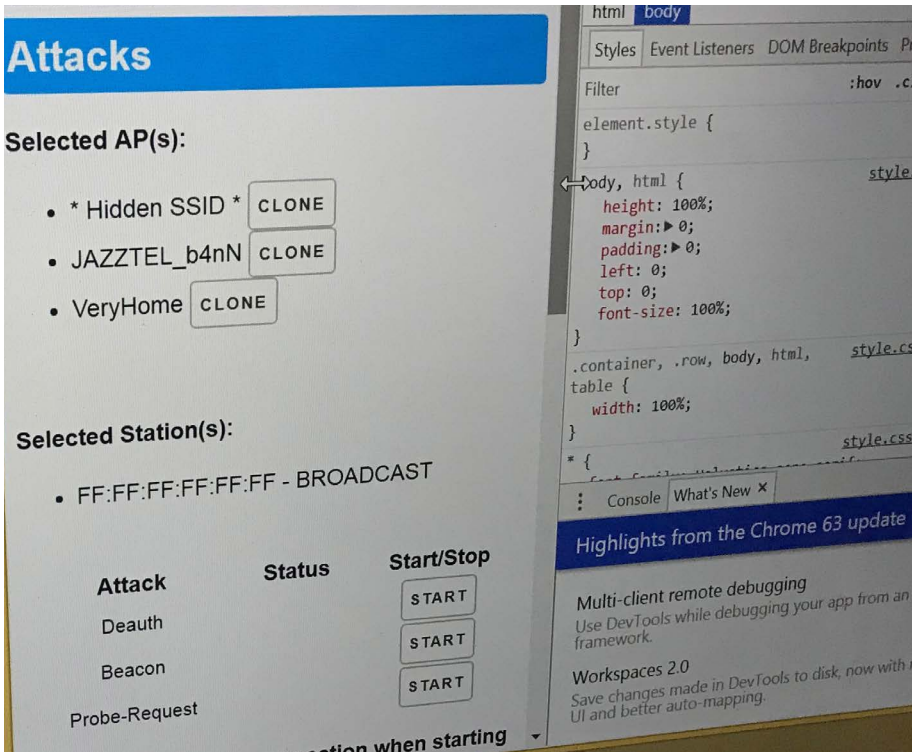


Fig. 33 Web severt NodeMCU ESP 8266

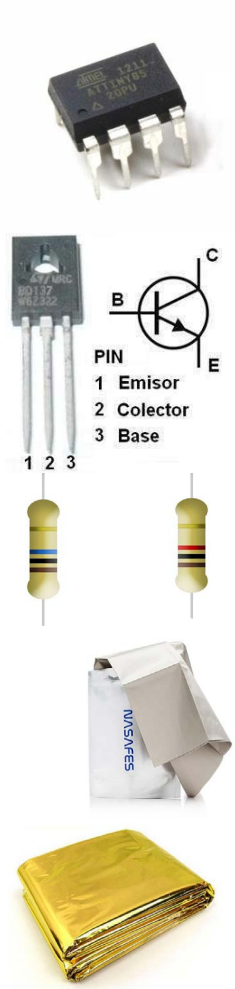


Fig. 34 ATtiny 85
Fig. 35 Transistor BD137
Fig. 36 Resistencias 1Mohm 1Kohm
Fig. 37 Téxtil NASAFES
Fig. 38 Manta Isotérmica

Conviene detallar los distintos componentes por separado:

- ATtiny85 es un microcontrolador programable, de bajo consumo, muy económico. Este microcontrolador responde con una señal lógica, se programa con una librería para que detecte cuándo el usuario toca el tejido conductor.

- Transistor BD137 funciona a modo de conmutador, permitiendo el paso de corriente que activa el relé y el Node MCU cuando se activa. Los relés son dispositivos electromagnéticos que funcionan como un interruptor controlado por un circuito eléctrico que, por medio de un electroimán, acciona los contactos que permiten abrir o cerrar otros circuitos independientes.

- Una resistencia de 10Mohm y una de 1kohm. Este un componente electrónico que produce una resistencia eléctrica entre dos puntos, permitiendo limitar la corriente o fijar la tensión.

- El tejido NSAFES ha sido usado como sensor capacitivo para poder detectar así al usuario al colocársela.

- La manta isotérmica ha sido diseñada para aislar y mantener el calor y dada su composición también evita la captura por visión térmica de algunos dispositivos de vigilancia.

El funcionamiento básico del wearable se inicia con la interacción del usuario. Al ponérselo, el microcontrolador ATtiny85 detecta un cambio significativo en los valores recogidos por el tejido conductor *NASAFES*, que actúa como sensor capacitivo del dispositivo. El microcontrolador ATtiny85 envía una señal lógica al transistor, que lo activa y hace que se cierre el circuito, permitiendo la circulación de corriente activando a su vez el Node MCU y el relé, este ultimo da paso a la activación paralela del *Jammer*. Este último ejecuta las instrucciones con las que ha sido programado y envía un ataque *deauthentication*. (DeAuth attack) a los dispositivos cercanos que usen tecnología WIFI, desconectándolos de sus respectivas redes y por otro lado mediante el jammer bloquea las conexiones; 3G, GPRS, GSM. De esta forma, con ambos dispositivos en funcionamiento creamos una especie de T.A.Z.

NODE ESP8266. Características

- CPU RISC de 32-bit: Tensilica Xtensa LX106 a un reloj de 80 MHz.

- RAM de instrucción de 64 KB, RAM de datos de 96 KB.

- Capacidad de memoria externa flash QSPI – 512 KB a 4 MB (puede soportar hasta 16 MB).
- IEEE 802.11 b/g/n Wi-Fi.

- Tiene integrados: TR switch, balun, LNA, amplificador de potencia de RF y una red de adaptación de impedancias.

- Soporte de autenticación WEP y WPA/WPA2.

- 16 pines GPIO (Entradas/Salidas de propósito general).

- Interfaz I²S con DMA (comparte pines con GPIO).

- Pines dedicados a UART, más una UART únicamente para transmisión que puede habilitarse a través del pin GPIO2.

- 1 conversor ADC de 10-bit.

El NODE MCU es una plataforma Open Source que lleva integrado un microchip ESP8266 para comunicaciones WiFi. Esta ha sido programada a partir de librerías OpenSource que hemos modificado para automatizar procesos que evitasen tener que acceder al servidor web para realizar las acciones de ataque y bloqueo de redes WiFi. En el momento en el que se activa se ejecutan una serie de acciones que, como hemos dicho, se han automatizado para que escanee las redes cercanas y a todos los clientes mediante un ataque *desauthentication* que desconecta todos dispositivos conectados al punto de acceso.

Este controlador, junto con el circuito inhibidor de redes móviles (3G, GPS, UHF), evita cualquier triangulación mediante los dispositivos móviles u otros *gadgets*. Con esto se busca adoptar el rol consciente de elemento invasivo, convertirnos en un sistema vírico (Expósito, 2005) como crítica a las políticas que han convertido tanto el espacio físico como el digital en un lugar fronterizo.

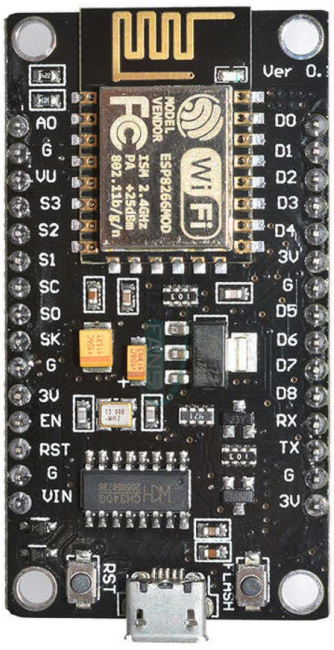


Fig. 39 NodeMCU ESP 8266

Jammer

Fig. 40 Camión militar de telecomunicaciones

Los dispositivos inhibidores comúnmente conocidos como jammer son generadores de señales que tienen la capacidad de interferir, saturar o bloquear las comunicaciones inalámbrica tales como llamadas, mensajes de texto, GPS, WIFI, servicio de datos, etc. Estos dispositivos constar, básicamente, de un oscilador que genera señales, un generador de ruido que mediante una etapa de potencia y una o varias antenas nos permite amplificar la señal y bloquear la comunicación entre el emisor de señales y el receptor.

Fig. 41 Estación Jammer

Para lograr interferir la señal debemos generar una señal que entre en resonancia con la frecuencia portadora, logrando así la inhibir la transmisión de datos. Estos sistemas inhibidores disponen de dos tipos de ataques de interferencia, que son utilizados para dificultar la comunicación de datos entre un emisor y el receptor. Estos ataques llevan el nombre de spot, un tipo de ataque direccionado a interferir en una frecuencia concreta, mientras que en el caso de ataques de tipo *barrage* se interfiere en varios canales simultáneamente. En cualquiera de ellos es necesario encontrar la frecuencia exacta para hacerlo efectivo y contar con la potencia necesaria para suplantar las señales originales.

Dependiendo del uso que se le quiera dar a estos dispositivos en el campo de la vigilancia podemos encontrar varios tipos de *jammers*:

Fig. 41 Jammer táctico

– *Vehículos Jammer*, usados frecuentemente en misiones militares o para cargos políticos con riesgo de atentado. Pueden bloquear dispositivos explosivos controlados por señales de radio. El rango de acción en este tipo de *jammer* difiere de los de uso más doméstico, disponiendo de antenas omnidireccionales de alta ganancia con un rango de acción entre 20Mhz y 3000Mhz y una potencia de 1600 vatios, proporcionando distancias de inhibición de hasta 100 metros.

– *Estaciones jammer*, usadas en instituciones penitenciarias, edificios militares, gubernamentales, parlamentos, embajadas, aeropuertos, etc. Al igual que los *vehículos jammer*, están orientados a protección contra artefactos explosivos controlados por radiofrecuencia, pero en este caso se busca evitar el tráfico de

información secreta. Este tipo de *jammer,* al igual que el anterior, tiene un alcance de larga distancia, pero con la diferencia de que puede interferir las frecuencias de manera simultanea o parcialmente según las necesidades.

Por último, están los *jammers* portátiles o tácticos, en los cuales nos hemos basado a la hora de la realización del dispositivo *CONTRA*. Estos dispositivos son usados generalmente por los agentes de control de aduana, negociadores de rehenes, artificieros, equipos de asalto, etc. Al igual que los anteriores pueden interferir en varías bandas de frecuencia, añadiendo las frecuencias VHF/UHF usadas en los buques y control de tráfico marítimo. Para más información, en los links relacionados al final del documento se encuentra toda la documentación revisada en este proyecto.

Antes de proseguir debemos nombrar dos de las obras que más han influido en *CONTRA; The Transparency Grenade* (2014) y *No Network* (2013) del artista e ingeniero Julian Oliver, cuya obra The Transparency Grenade gira en torno a la problemática de la guerra cibernética y la transparencia en los servicios corporativos y gubernamentales. El dispositivo creado por Julian Oliver toma la forma de una granada de mano F1 soviética con la intención de filtrar información de reuniones a puerta cerrada, capturando datos, audio, fragmentos de correo electrónico, páginas HTML e imágenes presentándolos en un mapa público en línea y mostrando la ubicación de su “detonación”.

Fig. 42 Julian Oliver. The transparency grenade. 2014

Fig. 43 Julain Oliver. No Network. 2013

5.3.2. Programación

Como hemos dicho anteriormente, hemos modificado el código original automatizando los procesos de ataque que genera el *WiFi deauth*, evitando de esta manera la necesidad de entrar al web server del NodeMCU, dando la facilidad de poder variar la cantidad tanto de paquetes enviados como la cantidad de usuarios a los que podemos atacar. Está preparado para interferir una banda de 2.4Ghz, pero remarco lo que ya hemos aclarado antes, no es una interferencia al uso, sino una saturación de los puntos de acceso con paquetes de datos.

A continuación, añadiremos primeramente de manera integra el código con las modificaciones del microcontrolador ATtiny85, ya que la extensión es mínima, y posteriormente el código empleado para el Jammer WIFI modificado, pero no el resto de las librerías, ya que eso excedería el número de páginas permitido en este documento. Toda la programación de la ATtiny85 se realizó mediante Arduino Nano.

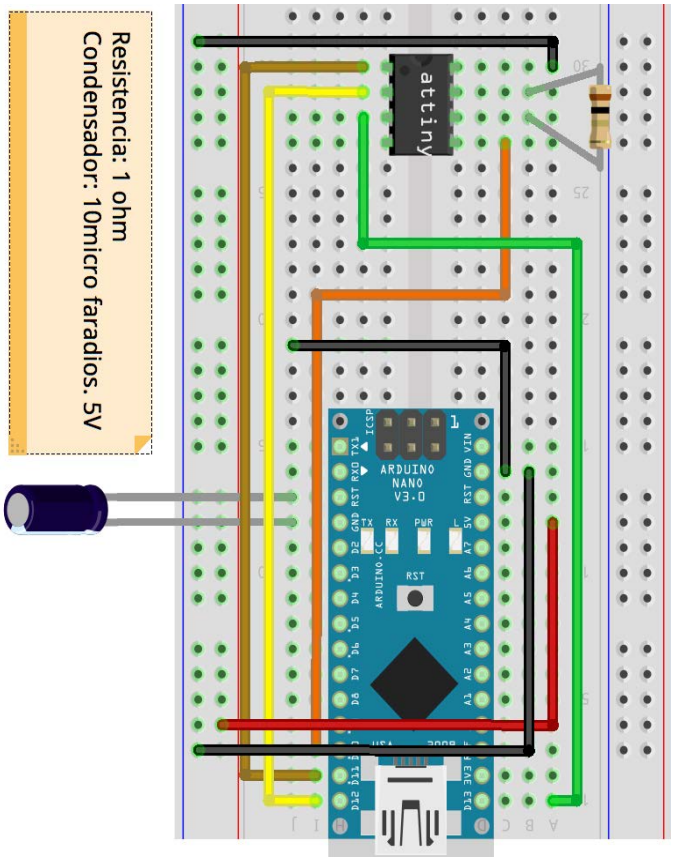


Fig. 44 Diagrama para programación de ATtiny 85

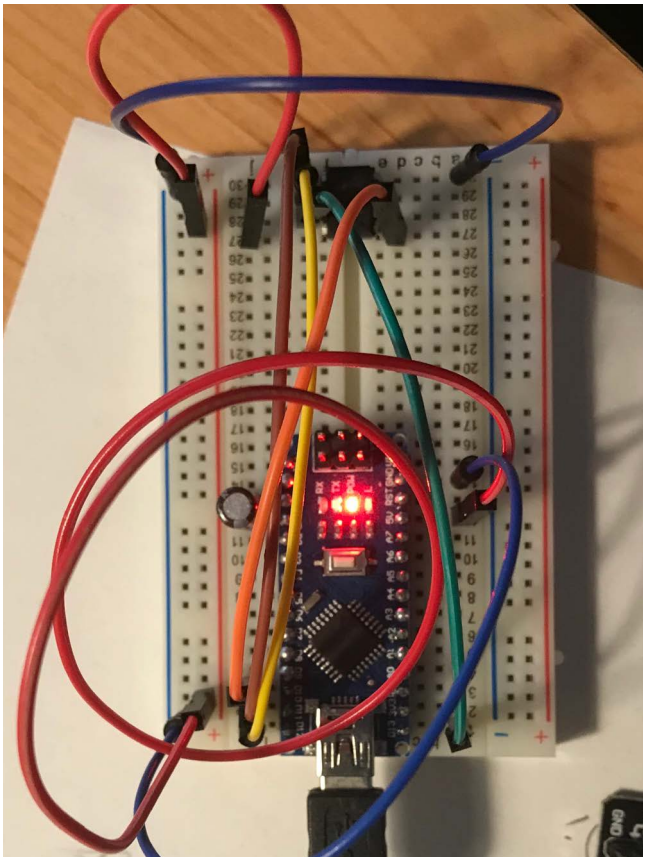


Fig. 45 Imagen circuito para programación de ATtiny 85

ATtiny

```
#include <CapacitiveSensor.h>

/*
 * CapitiveSense Library Demo Sketch
 * Paul Badger 2008
 * Uses a high value resistor e.g. 10M between send pin and receive pin
 * Resistor effects sensitivity, experiment with values, 50K - 50M. Larger resistor values yield larger sensor values.
 * Receive pin is the sensor pin - try different amounts of foil/metal on this pin
 */
 int led = 2;
CapacitiveSensor   cs_4_3 = CapacitiveSensor(4,3);        // 10M resistor between pins 4 & 3, pin 3 is sensor pin, add a wire and or foil if desired
/*CapacitiveSensor   cs_4_6 = CapacitiveSensor(4,6);        // 10M resistor between pins 4 & 6, pin 6 is sensor pin, add a wire and or foil
CapacitiveSensor   cs_4_8 = CapacitiveSensor(4,8);        // 10M resistor between pins 4 & 8, pin 8 is sensor pin, add a wire and or foil*/
 const long numReadings = 4; //numero de lecturas
 long readings[numReadings]; //arrray de las lecturas. Definiendo el tamaño del array
 int readIndex = 0; //puntero al indice actual. Le digo el lugar del array que va a modificar
 long total = 0;
 long average = 0; //average para hacer la media


void setup()

{

  cs_4_3.set_CS_AutocaL_Millis(0xFFFFFFFF);
  pinMode (2, OUTPUT);
     for (int thisReading = 0; thisReading < numReadings; thisReading++){
    readings[thisReading] = 0; //aquí inicializamos el array a 0. Reset


  }
```

```
}

void loop(){

    long actual =  cs_4_3.capacitiveSensor(30);

    total = total-readings[readIndex]; //restamos la ultima lectura
   readings[readIndex]=actual; //metemos en la posición de array actual el valor que obtenemos
     total = total + readings[readIndex]; //añade el valor actual al total
     readIndex = readIndex + 1; // marca la siguiente posición del array
     if (readIndex >= numReadings) readIndex = 0; //si ha llegado al final del array vuelve al principio
    average = total / numReadings; //calcula la media

 if (actual > average *2) {  //valor mayor que la media se multiplica
      digitalWrite (led, HIGH);
}else if (actual < average / 2){
           digitalWrite (led, LOW);
}


    /*

    if (actual > 1000)
      digitalWrite (led, HIGH);
      if (actual < 30)
           digitalWrite (led, LOW);




    /*} else {
      digitalWrite (led, LOW);
    }

    /*long total2 =  cs_4_6.capacitiveSensor(30);
    long total3 =  cs_4_8.capacitiveSensor(30);*/

     /*Serial.print(millis() - start);         // check on performance in milliseconds
    Serial.print("\t");                    // tab character for debug windown spacing
```

```
   Serial.print(actual);                // print sensor output 1
   Serial.print("\t");
   /*Serial.print(total2);               // print sensor output 2
   Serial.print("\t");
   Serial.println(total3);             // print sensor output 3*/

   delay(10);                          // tiempo para limitar los datos al
puerto serie.
```

A continuación, expondremos solo los fragmentos de código que se han realizado íntegros para la modificación del código original. Todos los archivos estarán en el repositorio de GitHub.

NODE MCU ESP8266

```
void loop() {

     //Parte añadida , capacitador apaga y enciende al
tocar-------------------
  //long start = millis();
  //long total1 =  cs_D8_D3.capacitiveSensor(30);

  //if (total1 > 10 && estado == 0){

    startAPScan(); // inicia el scan de puntos de acceso
    sendAPResults(); // enviá resultado del scan
   settings.multiAPs = true; //se habilita poder hacer una selección
múltiple de los puntos de acceso
   for (int i = 0; i < apScan.results; i ++) { // a partir de la lista, realiza
una acción con cada punto de acceso independientemente
      apScan.select(i); // esta es la acción del for, es la selección
de los puntos de acceso de modo automático
    }
    attack.stopAll();
    attack.start(0);
    startAttack();

  /*} else {
    attack.stopAll();
  }

 /* if(estado == 1){
    digitalWrite(LED_BUILTIN, HIGH);
  }
```

```
 if(estado == 1 && total1 > 400){
   estado = 2;
 }
 if(estado == 2){
   digitalWrite(LED_BUILTIN, LOW);
   //estado = 0;
 }

    Serial.print(millis() - start);          // check on performance in
milliseconds
   Serial.println("\t");                // tab character for debug windown
spacing

   Serial.println(total1);                // print sensor output 1
   */

   delay(10);                             // arbitrary delay to limit data to
serial port

 //---------------------------------

if (clientScan.sniffing) { // sniffing - rastrea las conexiones de
clientes
    if (clientScan.stop()) startWifi(); //si para el escan se activa el
wifi
 } else {
   server.handleClient(); //obetener cliente
   attack.run(); // y comienza el ataque
 }

 if(Serial.available()){
   String input = Serial.readString();
  if(input == "reset" || input == "reset\n" || input == "reset\r" || input
== "reset\r\n"){
     settings.reset();
   }
 }
```

5.3.3. Electrónica. Diagrama e imágenes

El proyecto consta de un circuito simple, con un total de 8 elementos electrónicos:

- 1 Node MCU ESP8266
- 1 Inhibidor de señales móviles

- 1 ATtiny85
- 1 Transistor BD137
- 1 Relé
- 2 Resistencias: 1K y 10M
- 1 Textil conductivo NASAFES
- 2 Manta isotérmica
- 1 PCB perforada
- Cables de conexión

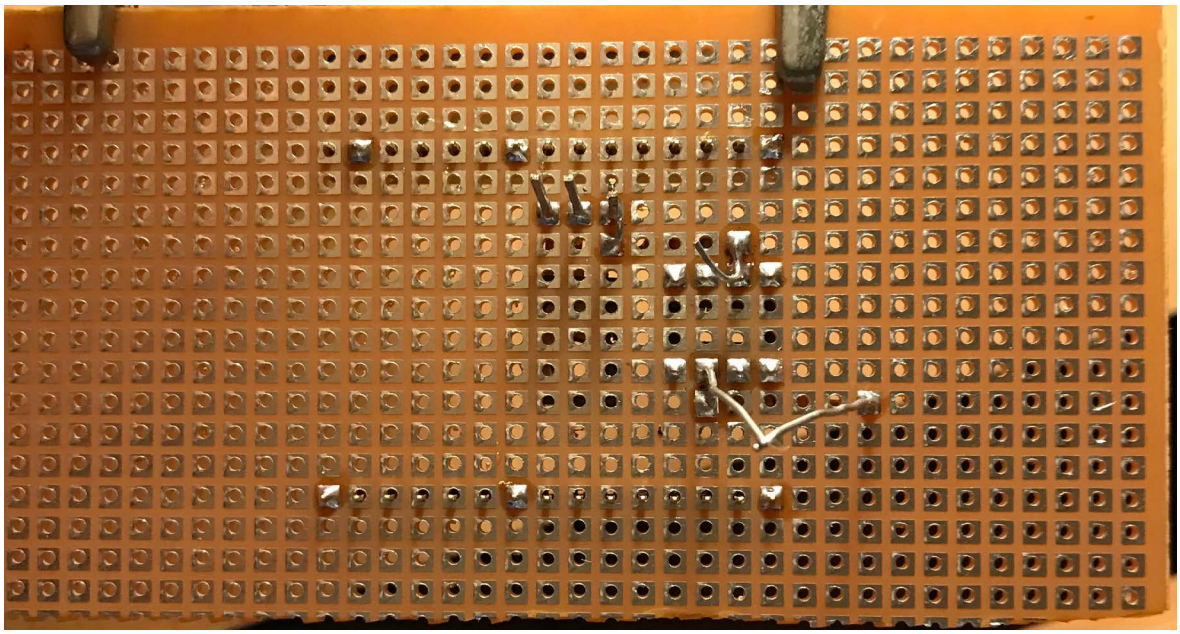


Fig. 46 Imagen de circuito. Cara A de placa perforada Inhibidor WIFI

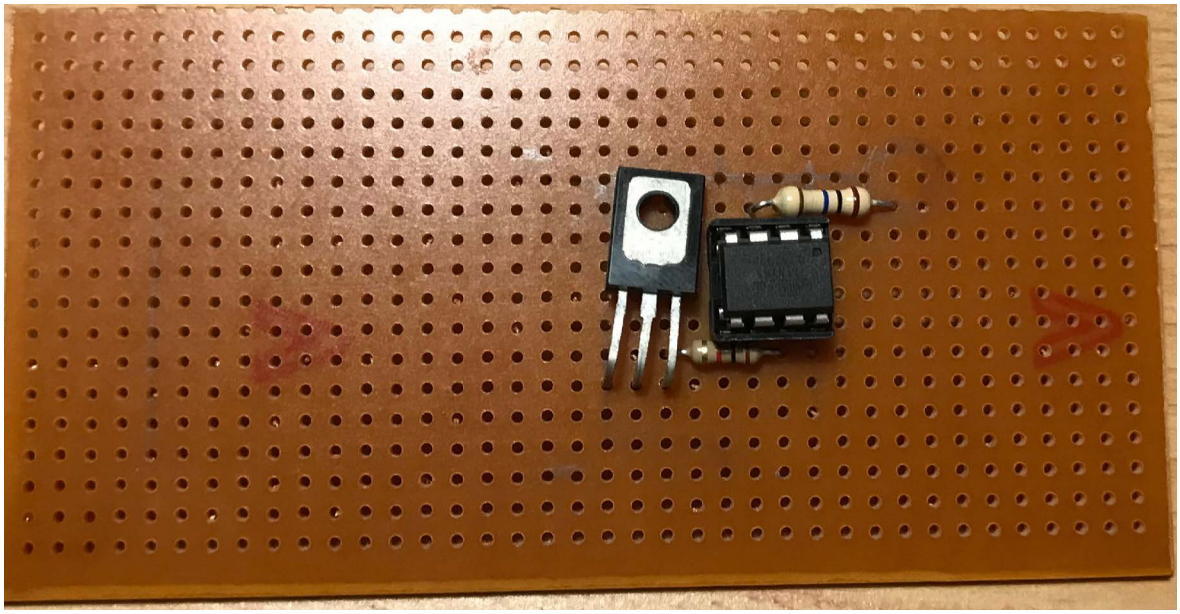


Fig. 47 Imagen de circuito. Cara B de placa perforada Inhibidor WIFI

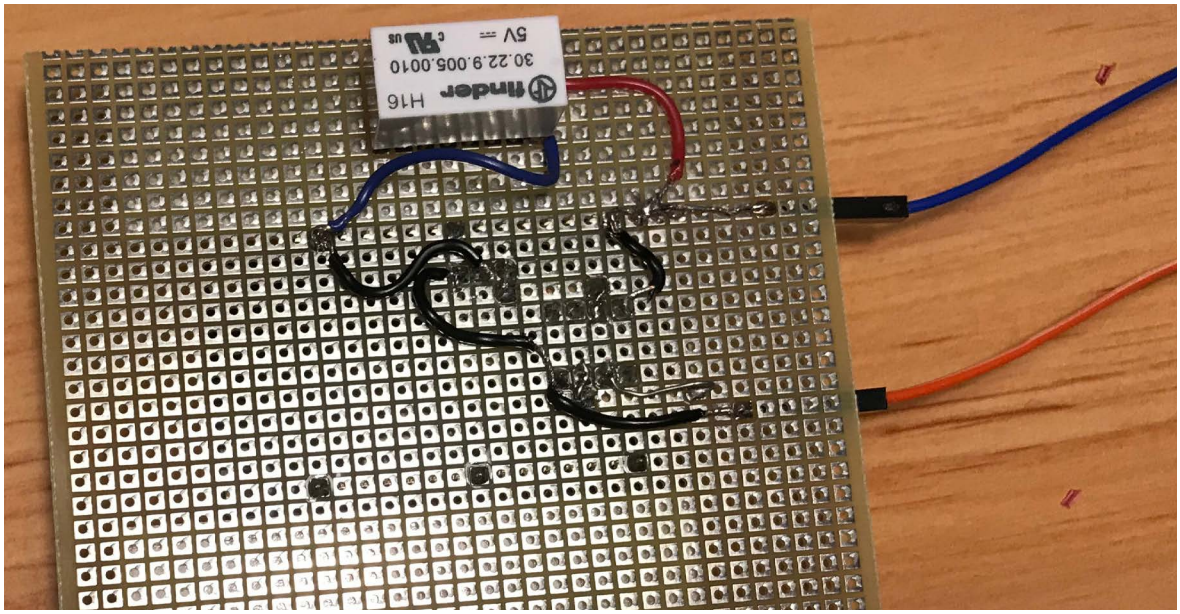


Fig. 48 Imagen de circuito. Cara A de placa perforada Inhibidor WIFI

Fig. 49 Imagen de circuito. Cara B de placa perforada Inhibidor WIFI

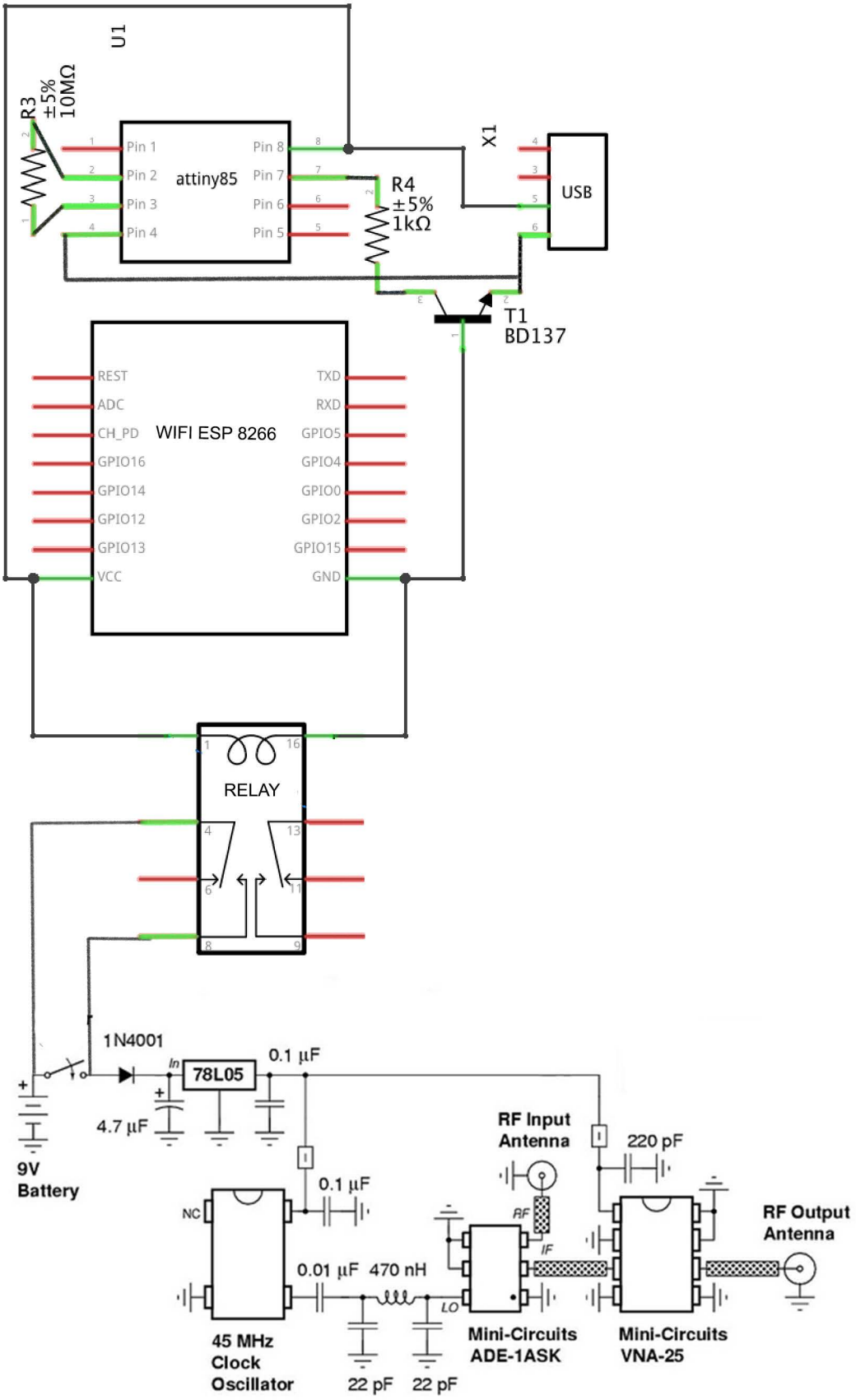


Fig. 50 Diagrama conexiones circuito inhibidor WIFI y circuito Jammer

5.3.4 Diagrama de interacción

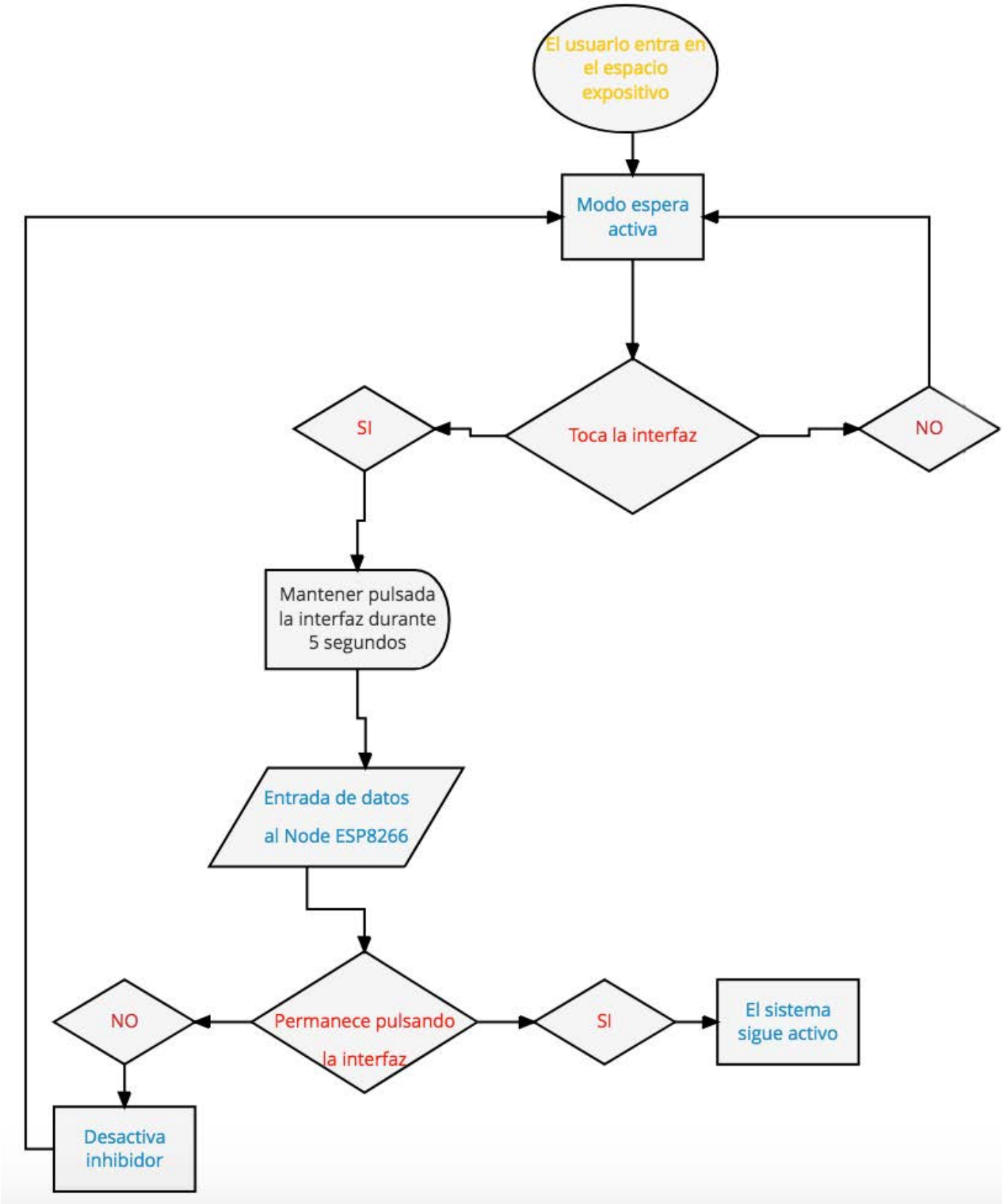


Fig. 51 Diagrama de interacción CONTRA

5.4. *CONTRA*. Exposiciones y acciones

Para las pruebas de campo en espacios públicos y privados tuvimos la suerte de poder exponer *CONTRA* en varias instituciones. Esto nos ha permitido comprobar las dinámicas que se producen entre los usuarios y la obra entorno al método expositivo, puesto que el *interfaz* está hecho con el propósito de ser utilizado o revisado de manera abierta.

A continuación, expondremos las imágenes de las exposiciones que se realizaron durante el 2018 y 2019.

Fundació La Posta. Valencia

Fig. 52 Exposición CONTRA. Fundaión La Posta. 2018

Fig. 53 Exposición CONTRA. Fundaión La Posta. 2018

En esta ocasión CONTRA se expuso suspendida del techo en el centro de la sala mediante nylon y una percha realizada con un tubo de cartón. Por cuestiones del espacio era el mejor método ya que permitía revisarlo entero, pero por la disposición en la que se encontraba colocado hizo difícil el que los usuarios pudiesen probárselo. Por este motivo se habilitó una extensión del tejido conductivo que permitía probar el funcionamiento al tocarlo con las manos.

Centre del Carme Cultura Contemporània. Valencia

Enmarcada dentro del Festival *Volumens Day* junto a varios compañeros de diferentes años del Máster de Artes Visuales y Multimedia, se expuso nuevamente CONTRA. En este contexto

por la dificultad para colgar el wearable como se hizo en la Fundació La Posta, se nos prestó un trípode con una adaptación en la parte superior que funcionaba como una percha.

Fig. 54 Exposición CONTRA. CCCC. 2018

La problemática en este espacio era similar a La Posta, pero con el añadido de que el trípode en contacto con el circuito hacía interferencias ocasionales activando el sistema inhibidor. Por parte de los usuarios, también fueron reacios a probarla si no había alguien presente para explicarles el proyecto. Otra observación que hicimos en este espacio fueron las interferencias que podían ocasionar la arquitectura, ya que según donde la onda que se propaga del inhibidor se veía reducida.

Fig. 55 Exposición CONTRA. CCCC. 2018

Escuela Técnica Superior de Ingeniería Informática de la Universitat Politècnica de València

Por último, en la escuela de ingeniería informática se expuso de un modo más didáctico. El warable se expuso montado en un maniquí pudiendo dar un poco más de acceso al propósito de probarlo por parte de usuario. Se acompaño se varias cartelas con el concepto del proyecto algunos diagramas y explicaciones sobre la electrónica. Claramente los usuarios que eran mayormente estudiantes de la escuela de informática mostraron un gran interés en el funcionamiento, llegando a explorar el wearble sin necesidad de estar alguien presente para comentar el proyecto.

Como hemos dicho en todos los casos pudimos experimentar con el formato expositivo y la interacción con los usuarios y el feedback que se produjo durante las exposiciones fue altamente interesante, ya que se mantuvo muchas conversaciones con

los interesados que aportaron una cantidad de información considerable respecto al tema: opiniones, discusión entorno al concepto, soluciones sobre electrónica, etc.

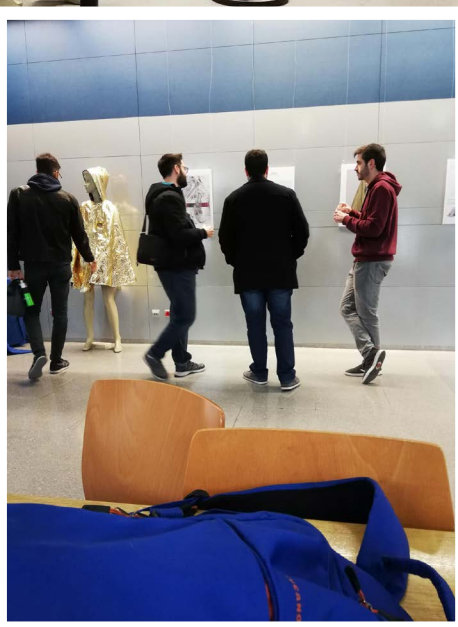


Fig. 56 Imagen superior. Exposición CONTRA. Etsi. 2019
Fig. 57 Imagen derecha. Exposición CONTRA. Etsi. 2019

Próximamente el proyecto estará exponiéndose en el festival Ars Electronica de Linz, donde podremos obtener un eco especialmente valioso, ya que el contexto en el que se expondrá se centra explícitamente en la relación arte-tecnología. Podremos aquí realizar una acción usando el wearable entre los asistentes produciendo el feedback para el que está concebido *CONTRA*.

Para finalizar esta investigación se adjuntan las imágenes de la acción realizada en el control de Aduanas del puerto de Valencia y la base aérea Militar de Quart de Poblet: lugares elegidos por su clara relación con los conceptos que se abordan en este documento.

Fig. 58 Imagen izquierda. Acción CONTRA. 2019

Fig. 59 Imagen izquierda. Acción CONTRA. 2019

Fig. 60 Imagen derecha. Acción CONTRA. 2019

Fig. 61 Imagen derecha. Acción CONTRA. 2019

6. Conclusión y trabajo futuro

Tras la finalización del prototipo CONTRA y la consecuente investigación realizada, esto nos ha ayudado a comprender las mecánicas y mecanismos del poder que se han instaurado en la modernidad, llevándonos a reflexionar sobre la relación que mantenemos con los dispositivos de comunicación y vigilancia y como permitimos que estos vertebren gran parte de nuestra vida diaria.

A través de una revisión de las prácticas artísticas contemporáneas centradas en el tema de la privacidad e invisibilidad digital, tanto con artistas que se han incluido como los que no en este documento, tales como: Pierre Derks, CV Dazzle, Naomi Wu, Simone C. Niquille, Becky Stern, Marcha Shagen y Leon Baaw, etc, se ha elaborado una crítica sobre la vigilancia que se ha materializado en el proyecto que aquí se presenta.

Cabe mencionar que el proyecto hace una revisión sobre el poder mediante conceptos teóricos y casos concretos de actualidad que ponen de manifiesto la problemática de los espacios fronterizos con la consecuente repercusión sobre las redes digitales de comunicación y el modo en el que los usuarios interactúan con estas.

Por otra parte, durante el proceso de trabajo y las correspondientes pruebas de campo durante las exposiciones y acciones se han analizado problemas a nivel de funcionamiento que se irán resolviendo en las próximas modificaciones, con la elaboración de circuitos de producción industrial, los cuales lograrán optimizar el funcionamiento del prototipo actual, que ha sido elaborado con los medios que se disponía por motivos económicos.

Pese a ello y las dificultades que han surgido en el proceso se ha logrado un funcionamiento altamente eficiente. En un futuro próximo se plantea realizar algunos workshops entorno al tema tratado, con la intención de que los usuarios puedan fabricarse sus propios wearables para la inmunidad digital. Finalmente, lo que aquí se ha creado solo es una de las muchas metáforas que pueden existir.

Conviene mencionar algunas de las ventajas del prototipo: la portabilidad y la capacidad de adaptación del proyecto en diferentes entornos y lo económico del resultado, puesto que

la producción no ha costado más de cien euros en materiales. Esto logra que prototipo sea reproductible a un bajo precio en cualquier lugar donde los sistemas de vigilancia estén integrados de manera cotidiana.

Somos conscientes de la dificultad que plantean este tipo de proyectos y la magnitud e importancia que los acompaña, pero esto nos ha permitido ir paso a paso escalando por una red compleja de cuestionamientos teóricos y de nuevos lenguajes, con los que hemos adquirido metodologías de investigación y herramientas que nos han abierto la posibilidad de realización de nuevos proyectos.

Actualmente está en marcha la producción de un prototipo de cámara para las redes sociales que haciendo uso de IA evitará la exposición de terceros en *selfies* ajenos. Este dispositivo lleva como nombre provisional Anti-Selfie y funcionará en tiempo real, es decir, haciendo uso de los accesos a cámara permitidos por los usuarios desde las propias redes sociales.

BIBLIOGRAFÍA

Monografías

Agamben, G. 2004. *Estado de excepción. Homo sacer II*. Buenos Aires: Adriana Hidalgo.

—2015. *¿Qué es un dispositivo? Seguido de El amigo y de La Iglesia y el Reino*. Barcelona: ANAGRAMA

Bauman, Z, y Lyon, D. 2013. *Vigilancia líquida*. Barcelona: Planeta.

Bazzicalupo, L. 2016. *Biopolítica. Un mapa conceptual*. Barcelona: Melusina.

Bentham, J. 1979. *El Panóptico. El ojo del poder*. Bentham en España. Madrid: La Piqueta.

Bellardo, J y Savage, S. 2003. "*802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions". Proceedings of the USENIX Security Symposium* – via Cal Poly https://www.usenix.org/legacy/events/sec03/tech/full_papers/bellardo/bellardo.pdf

Bey, H. 2014. *Zona temporalmente autónoma*. Madrid: Enclave.

Butler, J. 1997. *Mecanismos psíquicos del poder*. Teorías sobre la sujeción. Valencia: Universitat de València/Instituto de la Mujer.

Deleuze, G. 2006. *Conversaciones*. Valencia: Pre-textos.

Deleuze, G. 2004. *Mil mesetas. Capitalismo y esquizofrenia*. Valencia: Pre-textos.

Esposito, R. 2005. *Immunitas: Protección y negación de la vida*. Buenos Aires: Amorrortu.

Esposito, R. 2006. *Bíos. Biopolítica y filosofía*. Buenos Aires: Amorrortu.

Foucault, M. 1967. *"Des espaces autres"*, en *Architecture, Mouvement, Continuité* 1984

—1979. *Microfísica del poder*. Madrid: La Piqueta.

—1990. *Tecnologías del yo*. Barcelona: Paidós.

—2002. *Vigilar y castigar: nacimiento de la prisión*. Buenos Aires: Siglo XXI.

—2005. *Historia de la sexualidad. La voluntad del saber*. Buenos Aires: Siglo XXI.

—2014. *Las redes del poder*. Buenos Aires: Prometeo.

—2017. *Un diálogo sobe el poder y otras conversaciones*. Madrid: Alianza.

Gómez de Ágreda, Á. 2019. *Mundo Orwell. Manual de supervivencia para un mundo hiperconectado*. Barcelona: Planeta.

Han, Byung-Chul. 2018. *Sobre el poder*. Barcelona: Herder Editorial.

—2018. *Psicopolítica*. Barcelona: Herder Editorial, S.L.

Hobbes, T. (Sin fecha). *Leviathán*. https://omegalfa.es/downloadfile.php?file=libros/leviathan.pdf

Huxley, A. 2014. *Un mundo feliz*. Madrid: Tauro

Locke, J. 2005. *Segundo tratado sobre el gobierno civil*. Buenos Aires: Universidad Nacional de Quilmes/Prometeo.

Luhmann, N. 1977. *Ansätze zur analyse von match in der Politikwissenschaft*. Universitas. Zeitschrift fur wissen chaft, kubst ud literatur 5

Praiser, E. 2017. *El filtro burbuja. Cómo la red decide lo que leemos y lo que pensamos*. Barcelona: Taurus

Razac, O. 2015. *Historia política del alambre de espino*. Barcelona: Melusina

Rousseau, J. (Sin fecha) *El contrato social*. http://bibliotecadigital.ilce.edu.mx

Sauquillo, J. 2017. *Michael Foucault: Poder, Saber y subjetivación*. Madrid: Alianza.

Sloterdijk, P. 2017. *El desprecio de las masas*. Valencia: Pre-Textos.

Tiqqun. 2015. *La hipótesis cibernética*. Madrid: Acuarela.

Vamosi, R y Kevin Mitnick. 2018. *El arte de la invisibilidad. El hacker más famoso del mundo enseña técnicas de seguridad en la era Big Brother y Big Data*. Madrid: ANAYA.

Weizman, Eyal. 2012. *A través de los muros*. Barcelona: Errata naturae.

Weber, M. 2002. *Economía y sociedad*. Madrid: FCE.

Consultas Web

Eduardo Kac (consultado el 3 de noviembre 2016)

https://www.ekac.org/timec.html
https://www.ekac.org/figs.html

PRISM (consultado el 2 de enero 2017)

https://www.eldiario.es/turing/vigilancia_y_privacidad/vigilancia-espionaje-mundo-paises_0_144186025.html
https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data
https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data
https://es.wikipedia.org/wiki/PRISM
https://hipertextual.com/2013/06/que-es-prism-claves

Patrullas Ciudadanas en la frontera de México (consultado el 3 de mayo 2017)

https://www.laopinioncoruna.es/mundo/2009/03/24/miles-internautas-vigilan-frontera-eeuu-mexico-camaras-web/271287.html

The visual Watchers (consultado el 20 de agosto 2017)

http://www.rtve.es/fotogalerias/monstruos-maquina-frankenstein-siglo-xxi/185075/the-virtual-watchers-2016-joana-moll-cedric-parizot/13
http://www.antiatlas.net/joana-moll-cedric-parizot-the-virtual-watchers-en/
http://www.virtualwatchers.de/

Poder (consultado el 2 de octubre 2017)

https://definiciona.com/poder/

Wearables con GPS integrado (consultado el 20 de octubre 2017)

https://www.publico.es/ciencias/tecnologia/ropa-especial-protegerse-del-crimen.html
https://www.bladerunner.tv/catalogsearch/result/?q=GPS

JAMMER (consultado el 20 de octubre 2017)

https://es.wikihow.com/hacer-tu-propio-bloqueador-de-se%C3%B1al-de-celular

WickiLeaks, Assange, Manning y Snowden (consultado el 2 de enero 2018)

https://es.wikipedia.org/wiki/Julian_Assange
https://es.wikipedia.org/wiki/Chelsea_Manning
https://www.wikileaks.org/wiki/Afghan_War_Diary,_2004-2010
https://es.wikipedia.org/wiki/Edward_Snowden
https://www.20minutos.es/noticia/1850380/0/caso-snowden/cronologia/espionaje-ee-uu/

Antenas de radiofrecuencia e inhibidores (consultado el 3 de enero 2018)

http://microondasism.blogspot.com/2012/10/bandaism-lasbandas-ism-industrial.html
https://thesecuritysentinel.es/crea-tu-wifi-jammer-por-5-euros-y-con-arduino/

VHF, UHF, RFID y etiquetas RFID (consultado el 4 de enero 2018)

https://es.wikipedia.org/wiki/VHF
https://es.wikipedia.org/wiki/UHF
https://es.wikipedia.org/wiki/RFID
https://es.wikipedia.org/wiki/Etiqueta_RFID

The Critical Engineering Manifesto (consultado el 5 de enero 2018)

https://criticalengineering.org/es

Antenas de radiofrecuencia e inhibidores (consultado el 20 de enero 2018)

http://cecs.wright.edu/~pmateti/InternetSecurity/Lectures/WirelessHacks/Mateti-WirelessHacks.htm#_Toc77524675
http://users.csc.calpoly.edu/~bellardo/pubs/usenix-sec03-80211dos-html/aio.html

Joana Moll (consultado el 1 de febrero 2018)

https://mosaic.uoc.edu/author/joana-moll/

BioArtist (CAE) Steve Kurtz y Robert Ferrell (consultado el 5 de febrero 2018)

http://critical-art.net/
http://www.rebelion.org/noticia.php?id=13338
http://critical-art.net/siteapps/WordPress-49402/htdocs/defense/
https://vimeo.com/126806168

CAE: Desobediencia civil electrónica (consultado el 5 de febrero 2018)

https://sindominio.net/fiambrera/cae.htm
https://sindominio.net/fiambrera/simulacion.htm

Julian Olvier (consultado el 5 de febrero 2018)

https://julianoliver.com/output/transparency-grenade
https://transparencygrenade.com/

Apagar Internet y Yami-Ichi (consultado el 1 de enero 2019)

https://www.enriquedans.com/2009/09/el-gran-boton-rojo-que-apaga-internet.html
https://cargocollective.com/widephoto/Switch-Off-the-InternetThe-Influencers-FestivalClosed
https://retina.elpais.com/retina/2018/12/26/innovacion/1545832016_861025.html

USA Patriot Act (consultado el 5 de enero 2019)

http://interamerican-usa.com/articulos/Leyes/US-Patriot%20Act.htm
https://web.archive.org/web/20090216081628/http://www.lifeandliberty.gov/highlights.htm

American Border Patrol (consultado el 10 de Abril 2019)

https://www.efe.com/efe/usa/inmigracion/grupo-civil-presenta-sistema-para-vigilar-la-frontera-con-potentes-sensores/50000098-3676187
https://www.americanborderpatrol.com/
https://www.facebook.com/Seidarm/
https://www.youtube.com/watch?v=5nGy7mGzMnE

Frontera España-Marruecos (consultado el 10 de Abril 2019)

https://www.nytimes.com/es/2018/09/10/opinion-muro-migracion-europa/

ÍNDICE DE IMÁGENES