IV Congreso Chileno de Antropología. Colegio de Antropólogos de Chile A. G, Santiago de Chile, 2001.

Feos, sucios y malos. La imagen de los hackers en los medios de comunicación.

Pablo Gustavo Rodriguez.

Feos, sucios y malos. La imagen de los hackers en los medios de comunicación

Pablo Gustavo Rodriguez

Introducción: Objetivos y metodología

El presente trabajo constituye un informe preliminar de parte de una investigación en curso desarrollada en el marco de mi proyecto de tesis de doctorado que lleva por título "Una etnografía del Hackerdom en Argentina", bajo la dirección de la Dra. Virginia Ceirano, en la U.N.L.P.

El objetivo de este estudio es caracterizar la construcción discursiva acerca de los "hackers" en los medios de comunicación social argentinos. Para alcanzarlo se buscaron todas las notas periodísticas publicadas sobre los hackers, entre los años 1997 y 2000 en las ediciones electrónicas de los diarios argentinos en Internet cuya edición en papel es de circulación nacional. Así se constituyó un corpus integrado por 107 documentos que están siendo analizados mediante semiótica de enunciados con el programa NUD*IST© 4.

El marco metodológico es el análisis de discurso en su particular variante conocida como semiótica de enunciados (SE), desarrollada por el prof. Juan Angel Magariños de Morentín en varios textos, con algunos aportes del Análisis Crítico del Discurso (ACD) de Teun van Dijk. De acuerdo a la SE el sentido de los términos hallados en el discurso se construye en su uso, por lo cual no cabe suponer un sentido previo "correcto" sino analizar cuál es el que surge del contexto del discurso mismo. Al mismo tiempo se supone que todo decir efectivo se corresponde con una posibilidad de decir. En otras palabras antes que algo sea dicho existió, en esa determinada sociedad, la posibilidad de decirlo; fue un "mundo posible", en el sentido de la lógica modal.

El procesamiento de los textos comienza entonces con su normalización, segmentación y sometimiento a un proceso de reescritura a fin de reducirlos a un conjunto de enunciados denominados "definiciones contextuales" de los términos que interesan al analista. Estos archivos de enunciados constituyen las bases de datos para el análisis, cuyo objetivo es identificar las redes de enunciados (secuenciales y contrastativas) que permitirían la operacionalización del concepto foucaultiano de "formaciones discursivas".

El ACD, por su parte, considera al discurso como una forma de acción social, atravesada por relaciones de poder y realizando una labor ideológica en la que construye a la sociedad y a la cultura a la vez que es constituido por ellas. Por lo tanto el ACD procura realizar una trabajo interpretativo y explicativo de los problemas sociales a través del discurso (Norman Fairclough y Ruth Wodak En: van Dijk, Teun A 2000: 367 - 400). Asimismo van Dijk ha realizado una descripción muy esclarecedora de las macroestructuras y las superestructuras del discurso periodístico (van Dijk T. A. 1978, 1980) y tanto él como varios otros analistas e investigadores que siguen esta línea, han conducido estudios sobre el discurso racista en los medios de comunicación europeos (van Dijk T. A.1997, 2000) que revelan paralelismos interesantes con nuestros hallazgos sobre la construcción de un estereotipo del "hacker" en los medios argentinos.

Hallazgos

1. ¿Cómo designan los diarios a los hackers?

Aparte del mismo vocablo "hacker", utilizado en 98 de los 107 documentos analizados, los lexemas con los que se designa a los hackers, en orden de frecuencia son:

Nodo	Concepto	Docs.
(2 2 1)	Piratas, piratas informáticos, piratas cibernéticos, ciberpiratas. NOTA: Cabe recordar que la definición del diccionario de pirata incluye el concepto de ladrón ("ladrón que roba en el mar"), así como el de "clandestino" y "sujeto cruel y despiadado".	67
(2 2 3)	cibercriminales, delincuentes cibernéticos, delincuentes tecnológicos	13
(2 2 2)	terroristas cibernéticos	7
(2 2 5)	vándalos informáticos	3
(2 2 4)	CiberRobin Hoods	1
(2 2 6)	alimañas informáticas	1
(2 2 7)	programadores	1
(2 2 8)	nueva guerrilla	1
(2 2 9)	diablos cibernéticos	1
(2 2 10)	saboteadores informáticos	1

Como puede apreciarse, todos ellos, con la sola excepción de "programadores" tienen connotaciones negativas.

2. TEMAS: ¿Qué tipo de acciones de los hackers salen en los diarios?. ¿Qué dicen los diarios que hace un hacker?

Lo siguiente es un listado de las acciones que las notas periodísticas atribuyen a los hackers, también por orden de frecuencia de mayor a menor.

Nodo (2 3) Conceptos/Acciones/

Nodo	Nombre y definición	Docs.
(2 3 9)	atacar, agredir, dañar; computadoras, redes, sistemas.	53
(2 3 9)	atacar, agredir, dañar; computadoras, redes, sistemas.	53
(2 3 8)	ingreso o penetración ilegal o no permitida en computadoras, redes o sistemas informáticos.	48
(2 3 2)	robar (dinero, tarjetas de crédito, códigos o información)	34
(2 3 1)	invadir o violar sistemas (computadoras o redes)	22
(2 3 3)	Falsificar, modificar o alterar datos o información.	19
(2 3 12)	provocar pérdidas económicas o gastos de dinero a terceros	17
(2 3 17)	realizar espionaje, espiar, fisgonear, curiosear, acceder a información ajena confidencial.	16
(2 3 31)	bloquear sitios web	14
(2 3 20)	destruir sistemas o información	14
(2 3 23)	hacer daño	9
(2 3 4)	demostrar la vulnerabilidad de los sistemas	9
(2 3 29)	atacar a usuarios comunes	8
(2 3 11)	realizar sabotajes	7
(2 3 13)	desestabilizar a las grandes empresas	7
(2 3 32)	expresar consignas políticas	7
(2 3 6)	cometer fraudes	6
(2 3 10)	estafar	6
(2 3 27)	ordenar o intentar ordenar acciones militares	6
(2 3 16)	crear programas dañinos	5
(2 3 22)	tomar venganza	5
(2 3 21)	extorsionar	3
(2 3 7)	delinquir	2
(2 3 18)	realizar una guerra informática	2
(2 3 19)	engañar	2
(2 3 33)	control remoto de computadoras	2
(2 3 5)	bloquear centrales telefónicas	1
(2 3 15)	piratear software y venderlo	1
(2 3 24)	trabajar a sueldo para criminales	1
(2 3 25)	burlarse de Bill Clinton	1
(2 3 26)	crackear	1
(2 3 28)	llamar la atención mediática	1
(2 3 30)	traficar con información robada	1
(2 3 34)	crear virus	1
(2 3 35)	efectuar escuchas telefónicas	1
(2 3 50)	Legales: Actividades permitidas por la ley, no delictivas y no dañinas.	25

Las actividades "Legales" (Actividades permitidas por la ley, no delictivas y no dañinas) que se les atribuyen son las:

Nodo	Nombre y definición	Docs.
(2 3 50 13)	Consultor privado en seguridad informática.	13
(2 3 50 11)	Colaborar con las autoridades, con la policía o el gobierno para detener a otros hackers o mejorar la seguridad de los sistemas informáticos.	10
(2 3 50 6)	Contribuir a defender o incrementar la seguridad, inviolabilidad o invulnerabilidad de los sistemas informáticos.	6
(2 3 50 1)	Evitar que otros hackers ingresen a los sistemas.	4
(2 3 50 2)	Encargados de la seguridad, Contratados por empresas u organismos estatales como auditores o como responsables de la seguridad de sus sistemas.	4
(2 3 50 3)	Dirigir organismos o fundaciones	2
(2 3 50 12)	Evitar la fuga de datos	2
(2 3 50 4)	Realizar Congresos	1
(2 3 50 5)	Defensa de privacidad	1
(2 3 50 7)	Detectar los puntos vulnerables de un sistema	1
(2 3 50 8)	Solidarias (crear páginas web para org. de DDHH)	1

Como vemos, la gran mayoría de las actividades atribuidas a los hackers son delictivas. Menos de un 25% de los documentos hacen alguna referencia a la realización de actividades no delictivas, y aún éstos no constituyen una reivindicación de los hackers sino que estas actividades legales son presentadas como una rareza, como algo fuera de la norma, o como un indicio de que los sujetos que las realizan han "sentado cabeza" y se han "pasado al bando contrario" abandonando el hacking, o sea que son relizadas por "ex-hackers".

3. *¿A quiénes atacan? (Blancos)*

(2 3 9 1) Los hackers son noticia por atacar los sistemas informáticos de Bancos, tarjetas de crédito, aerolíneas, grandes empresas (Yahoo!, Amazon, Excite, E-Bay, CNN, eTrade y Buy.com.), sitios del gobierno (Pentágono, CIA, FBI, Dto. de Defensa de los EEUU, ejército, marina y Fuerza Aérea, ministerios, Senado, Casa Blanca, Centro Nacional de Protección de la Infraestructura, NASA), ediciones electrónicas de los diarios más importantes del mundo y proveedores de Internet.

Por otra parte con frecuencia se señala que éstos son los "blancos" preferidos por los hackers. Sin embargo las notas también sugieren que pueden atacar a cualquier usuario. Incluso un artículo que comienza afirmando explícitamente que es altamente improbable que la PC de un usuario común resulte atacada por hackers dedica todo el resto de su espacio a alertar a esos usuarios sobre las diferentes formas en que su sistema podría ser atacado y recomienda protegerse usando antivirus y firewalls. Esta nota lleva por título precisamente "Cómo defenderse de los hackers". Los títulos de las otras notas que sostienen que "cualquier PC" puede ser atacada por los hackers son:

"Hábitos que cuidan"; "Tengo un hacker en mi teléfono celular" ; "Un atento centinela contra virus y hackers"; "A prueba de hackers"; "Espionaje.com"; "Peligro en el disco rígido" y "Según un hacker, "es como enfrentarse a un Goliat".

4. *¿Por qué lo hacen? (Motivaciones atribuidas y declaradas)*

Las motivaciones afirmadas y negadas por los individuos citados como hackers o especialistas son las siguientes:

No es para ganar dinero.
No es para impedir las ganancias de las empresas.
La intención es hacer una demostración de poder.
Demostrar lo inseguros que son los sitios de comercio electrónico.
Es por el desafío de vencer los sistemas de seguridad informáticos supuestamente inviolables. Para ver si son capaces de superar las vallas que un experto en seguridad informática puso.
Satisfacer la curiosidad.
Aprender cosas nuevas.
Buscar la vulnerabilidad de los sistemas de computación "no para aprovecharse de ellos, sino para señalar-

les a los expertos en seguridad informática los flancos débiles, para que puedan arreglarlos".
Descubrir fallas en Internet con la intención de prevenir al público.
Las motivaciones atribuidas por los autores de las notas son:
Por diversión. "Su desafío es vencer sistemas de seguridad informáticos supuestamente inviolables, y divertirse espiando, alterando o destruyendo DATOS DE ACCESO RESTRINGIDO".
Cobrar venganza por las investigaciones que lleva a cabo el FBI sobre los hackers o contra un antiguo empleador.
Como un juego.
Ver hasta qué punto llegan sus habilidades.
Demostrar que no existe un sistema infalible.
Un deporte de moda.
Lucrar con la venta de información robada en sus accesos no autorizados.
Adicionalmente, en la nota "CZ_Guerra desde los teclados" se presentan tres hipótesis, sin abogar por ninguna de ellas en forma especial:
Se trata de unos jóvenes fascinados por desplegar su anónimo poder, hoy seguramente muertos de risa
Una versión aggiornada de los luddistas, esos antiindustrialistas que rompían las máquinas
Un ensayo general y a gran escala de gangsterismo y guerra comercial
La estrategia discursiva más frecuente en lo que respecta a este tema consiste en poner en boca de algún entrevistado (hacker u otro especialista en informática) las declaraciones que atribuyen motivaciones altruistas, románticas o no-delictivas a los hackers, a fin de que el autor pueda tomar distancia de ellas, para, seguidamente, refutarlas, contradecirlas o ponerlas en duda mediante ejemplos que supuestamente las contradicen o bien mediante simples comentarios sarcásticos.

Psicología / Personalidad (trastornada) del hacker
El estereotipo del hacker, diferente a los jóvenes "normales", también es construido como presentando una personalidad enferma, trastornada, caracterizada por los siguientes rasgos:
ANTISOCIAL: en su mayoría son adolescentes pero consideran a su novia como su peor enemigo, al revés que el adolescente normal.
COMPORTAMIENTO OBSESIVO: quieren tener el 100% del tiempo para dedicarlo a la computadora.
SADISMO: Se divierten "espiando, alterando o destruyendo DATOS DE ACCESO RESTRINGIDO" ."Este muchacho que aprieta una tacita de telgopor entre los dedos dice: -Poné Serial Killer, que muchos van a llorar." "mezcla de técnicos anarquistas y científicos obsesivos"
PREPOTENCIA: "La información debe ser libre y gratuita, dicen, prepotentes"
IDOLATRÍA Y FETICHISMO: "y rinden culto al mismo dios: un disco rígido -no siempre el propio- preñado de información jugosa, que se abre como un durazno maduro".
COMPORTAMIENTO DESTRUCTIVO COMPULSIVO: "Pero Serial Killer no es su verdadero nick, aunque ilustra bastante bien un tipo de comportamiento compulsivo que le hizo verter sangre de computadoras hace un par de años. Doscientas o trescientas víctimas borradas a cero."
Algunos de estos rasgos se ilustran extensamente mediante relatos y anécdotas muy vívidos pero de dudosa veracidad, nunca verificables, de fuente anónima, muy afines a las conocidas "leyendas urbanas". A continuación citamos sólo un par de ejemplos por falta de espacio, para ilustrar su uso en la construcción de estereotipos.

Leyendas urbanas

ON-LINE DOCUMENT: LN_Peligro en el disco rígido

Text units 62, 64-68:
"Spock es de esa clase de personas que revuelve la basura. Hace poco logró hackear la máquina de la abogada del banco Almafuerte y encontró documentación que lo hizo dar un respingo de placer. Dice de sí mismo que no es normal. Que siente que hay algo enfermo. Cuando lo invitan a jugar al fútbol, corre un minuto treinta y sale disparado a buscar el árbol más próximo, para esconderse del sol. Apenas tiene 20 años. 62
-Llego a mi casa, me meto en mi pieza, enciendo la máquina y después prendo la luz. Es enfermo. 64
Spock es una criatura de pesadilla. Muchas de sus noches las pasó enterrado hasta las narices en computadoras ajenas, con una orden de borrar todo en la pantalla y jugando con sus amigos a acertarle con una goma de borrar a la tecla de Enter. 65

- El destino de un servidor dependía de la trayectoria de una goma de borrar, brotado de lujuria informática. 66
  Se llama Lobo. Es un tierno hacker de 16 años, que empezó a los 10. Se siente un bicho raro en el colegio. No entiende por qué a sus compañe-

ros no les apasionan los secretos que guarda un teléfono celular. Por qué ver el animalito destripado, estirando la antenita, no les produce un cosquilleo de emoción. 67

- Me gustan las máquinas porque me dan la posibilidad de expresarme -dice-, de hacer algo productivo sin ningún gasto. Con una computadora no necesitás bienes materiales y podés tener logros muy grandes... ¡Podés inventar un algoritmo! Pero el caldo vicioso de la información desborda las venas. Las rompe. Las tritura. Las deja secas. 68

Criminalización

Además de definirlos por la realización de acciones a las que se señalan como delitos, a pesar de que no están legalmente prohibidas ni penalizadas, y además de referirse a ellos como cibercriminales y ciberdelincuentes y de señalar entre sus actividades el robo de dinero y de información se criminaliza a los hackers utilizando un vocabulario policial e incluso militar para describir sus actividades y la respuesta a ellas por la policía.

a) Uso de vocabulario militar:

Por ejemplo, al describir las actividades de los hackers se las refiere como "ataques masivos", "ataques coordinados", "el golpe más audaz de toda su historia", "invasiones cibernéticas", "atentados", "una nueva forma de guerrilla". Para restar importancia a los ataques de denegación de servicio sufridos en febrero del 2000 a varios sitios de comercio electrónico el entonces pte. de los EEUU, Bill Clinton dijo que no eran "un Pearl Harbor electrónico".

A ellos se los identifica como "el enemigo" y como "un ejército subterráneo relacionado con los anarquistas que se enfurecieron tan espectacularmente con la Organización Mundial de Comercio en Seattle". Se los considera un "riesgo" o "amenaza para la seguridad nacional". Cuando un sistema resulta infectado por un virus se dice que "cayó en las garras del enemigo".

Las computadoras que utilizan son denominadas "plataforma de ataque" o "engranajes de un arma". Las ciudades donde viven o las empresas donde trabajan son llamadas su "centro de operaciones". Las computadoras que atacan son denominadas "blancos", "objetivos" o "víctimas". Sus "ataques" son considerados como un problema de seguridad nacional que motiva "reuniones cumbre" del presidente de los EEUU, con asesores en seguridad nacional con miras a definir "estrategias de defensa", "declarar una ofensiva", "dar batalla" o "declararles la guerra"

P. ej.: "La Agencia de Defensa Nacional comenzara la construcción de un sofisticado sistema de seguridad para prevenir las invasiones cibernéticas" (CD_De Japón hasta Perú...UT2)

"Pero la fuerte ofensiva del gobierno norteamericano parece no atemorizar a los piratas de la red, que AYER VOLVIERON A ATACAR" (CD_El FBI dice que los hackers... UT11)

Dichos "ataques" consisten en "el BOMBARDEO DE GRAN CANTIDAD DE INFORMACIÓN". Sus "armas" son troyanos, gusanos, cookies y computadoras.

Los programas y medidas de seguridad informática como los firewalls y antivirus son llamados "artillería contra los hackers".

b) Uso de vocabulario policial o penal

Frecuentemente se habla de los hackers en la prensa en relación a procesos judiciales o persecuciones policiales, por lo que abunda en estos casos el vocabulario policial, reforzando su imagen de delincuentes aún cuando no se los llame así abiertamente.

Por ejemplo se dice que "dieron un golpe" o se los menciona perseguidos por la policía, o el FBI, en procesos judiciales, con causas pendientes, en libertad condicional, prófugos de la justicia, siendo interrogados por la policía, recibiendo condenas de prisión, pagando fianzas o multas, siendo condenados a realizar servicios comunitarios, a tomar cursos de ética, o a verse privados del uso de computadoras.

A pesar de que reiteradamente se menciona al hacking como un delito en ocasiones se aclara que legalmente no está tipificado como tal y que por lo tanto la única manera de encarcelar a un hacker es esperar a que cometa algún otro delito tipificado, como robo de tarjetas de crédito, de líneas telefónicas, de dinero, fraude, estafa, extorsión, falsificación de información o privar a terceros de su derecho de acceso a la información.

Estrategias discursivas del habla racista

Como adelantamos al comienzo de este trabajo su carácter es preliminar y predominantemente descriptivo, pues el análisis de los datos aún no está concluido. Sin embargo, nos pareció que los datos recogidos hasta el momento eran suficientemente reveladores como para comunicarlos a los colegas que trabajan en temas relacionados y debatirlos. Por otra parte, varios estudios empíricos realizados sobre el habla racista en Europa en la línea del ACD presentan algunos paralelismos con nuestros propios hallazgos que consideramos importantes señalar.

Estos estudios definen al habla racista en sentido amplio como aquella forma de expresión y comunicación persuasiva de las actitudes e ideologías polarizadas que nos presentan a "nosotros" como buenos y a "ellos" como malos. Nosotros podríamos así considerar a las noticias analizadas sobre los hackers como un ejemplo de habla racista aún cuando el grupo presentado en términos negativos no se recorte por su pertenencia a una raza o grupo étnico diferente sino por otras características. Los mencionados estudios han encontrado las siguientes estructuras discursivas como significativas para la vehiculización del prejuicio.

Los temas: A diferencia del discurso sobre "nosotros" no encontramos aquí la habitual variación de temas sino una breve lista de "temas étnicos" preferidos, como la inmigración, el crimen, las diferencias y desviaciones culturales, la discriminación y los problemas socioeconómicos. El análisis de las proposiciones temáticas, por su parte, indica que éstas suelen tener implicaciones negativas. La inmigración, por ejemplo, nunca aparece tematizada como una cuestión neutra (...) sino como un grave problema, cuando no como un fraude, una invasión o una amenaza contra "nosotros". El delito aparece invariablemente entre los cinco temas étnicos más frecuente (a menudo en primer lugar).

Incluso cuando las minorías (en especial los negros) aparecen representados en forma más positiva, como en las noticias sobre deportes o espectáculos, se las categoriza en términos estereotipados. Las diferencias culturales suelen exagerarse y mostrarse como desviaciones de las normas y valores occidentales dominantes.

En lo medios de difusión los temas normalmente se expresan en los titulares y los artículos principales. La prensa, por medio de los temas de sus titulares, define la "situación étnica" en la que "ellos" constituyen un problema, cuando no una amenaza.

Como hemos visto en la exposición parcial de los resultados, el delito es el tema que ocupa el primer lugar en las noticias sobre los hackers, quienes son casi siempre retratados en términos negativos, como personas peligrosas, dañinas por naturaleza, de las que todos deben cuidarse.

La semántica local Hay una serie de mecanismos bastante típicos del habla racista que combinan las estrategias generales de presentarse a uno mismo en términos positivos (autopresentación positiva) y presentar a los demás en términos negativos (heteropresentación negativa). Uno muy conocido es el de la negación aparente, en el que a una cláusula inicial positiva en la què se niega el prejuicio o el racismo le sigue una cláusula adversativa que invariablemente expresa o implica algo negativo acerca de las minorías, como en la clásica frase "no tenemos nada acerca de los negros, PERO...". Este mecanismo se denomina de "negación aparente" debido a que la negación es inmediatamente refutada por las cláusulas siguientes, o incluso por todo el resto del discurso. En las noticias analizadas hallamos un mecanismo similar cuando se afirma que los hackers no roban ni destruyen información como los crackers, que su móvil es la curiosidad, pero a continuación se exponen teóricamente o mediante anécdotas las técnicas de robo y destrucción de información que se atribuyen a los hackers y se recomienda a los usuarios que se protejan de ellos.

Análogamente podemos encontrar una concesión aparente cuando reconocemos que hicimos algo malo (o que ellos hicieron algo bueno), pero luego disculpamos o minimizamos nuestra mala acción, o insinuamos que la de ellos no fue tan buena, después de todo.

Otro mecanismo es el de la transferencia: donde se atribuye el racismo a otro para exculparse uno mismo, p. ej. "Yo no tengo nada contra los negros, pero mis clientes ...". También de estos mecanismos hay ejemplos en nuestra base de datos.

Estilo: el estilo es el resultado de elecciones que realiza el hablante entre las opciones que tiene disponibles. Es una indicación o señalador de las proposiciones sociales de los hablantes y de la situación sociocultural del hecho del habla y tiene que ver básicamente con la posibilidad de decir "lo mismo" de diferentes maneras. Así, al poder optar entre varias alternativas posibles la elección de una forma en detrimento de otras revela información sobre el posicionamiento del enunciador respecto de su objeto de enunciación.

Los lexemas utilizados para denominar a los hackers, como "piratas", "delincuentes informáticos", "cibercriminales", "nueva guerrilla" y "terroristas cibernéticos" es reveladora de la actitud que los autores de esas notas tienen ante el grupo en cuestión.

Asimismo, mediante el uso de pronombres, los hablantes pueden indicar su pertenencia al grupo con el que se identifican y acentuar su distancia social, su desaprobación o su resentimiento respecto de las minorías. La oposición fundamental entre nosotros y ellos es un ejemplo clásico y muy conocido. Esto también se manifiesta mediante el uso de demostrativos, como en "esa gente". El uso de las comillas para permitir al enunciador poner en boca de otros los que él mismo no puede o no desea decir. Además de la precisión, la vivacidad o la efectividad dramática, puede decirse que las citas se utilizan a menudo para establecer una distancia entre el periódico y la persona o las opinio-

nes citadas. En nuestros datos, hemos visto cómo se ponen entre comillas como una cita de otros todas las "heteropresentaciones positivas" de los hackers, casi siempre en boca de los mismos hackers. El uso de verbos comunicacionales expresan a veces la evaluación del cronista sobre el contenido de lo que dice el hablante: en nuestro caso "Ellos dicen que no son delincuentes...".

Conclusiones provisorias

Podríamos preguntarnos ¿por qué los medios se expresan de este modo sobre los hackers?. Tal vez sea muy prematuro esbozar una respuesta, pero por lo pronto pensamos que puede tener que ver con los valores periodísticos. Nos referimos con ellos a los que determinan la posibilidad de que un hecho sea seleccionado para ser formulado como noticia y publicado. En primer término están los formulados en términos económicos: las creencias y opiniones de poderosos actores de la noticia (las fuentes), de los anunciantes, los suscriptores, etc. En segundo lugar están la rutinas sociales de recopilación de las noticias y la producción organizativa, derivada de la periodicidad de publicación, accesibilidad de las fuentes, etc. Estos hacen que se favorezca la selección y producción de relatos periodísticos sobre las elites y que reflejan los valores económicos, sociales e ideológicos de esas elites. Pero en tercer lugar tras haber pasado por los filtros anteriores hay toda una serie de limitaciones cognitivas más específicas que definen los valores periodísticos sobre lo que es digno de ser considerado una noticia y publicado. Los estudios europeos mencionados más arriba señalan que entre éstos valores están la novedad, la actualidad, la presuposición, la consonancia, la relevancia, la proximidad, la desviación y la negatividad.

Varios estudios de comunicación, semiótica, cognición y discurso destacan la importancia que la prensa tiene en la formación de estereotipos sociales, esquemas mentales o modelos situacionales y, consecuentemente, de actitudes sobre grupos minoritarios o en algún sentido "diferentes" a la mayoría, como podría ser el caso de los hackers.

Un gran número de estereotipos para los grupos y, en particular, para las nacionalidades o grupos raciales se basan en poco o ningún conocimiento personal de primera mano. Se derivan del medio o entorno social con poca oportunidad para contrastarlos o modificarlos mediante el contacto personal directo.

Un problema de los estereotipos sobre la gente es que, una vez aplicados, son difíciles de compulsar y corregir. Es relativamente fácil descubrir si los perros tienen tres patas en vez de las cuatro previstas: basta con mirar el caso discrepante. Pero no es fácil determinar si es o no apropiado un conjunto particular de rasgos de personalidad. Debido a que las expectativas guían en gran medida la percepción y la interpretación y debido a que las motivaciones de la conducta son generalmente ambiguas, los estereotipos preexistentes sobre los individuos pueden inducirnos automáticamente a percibir esos rasgos, incluso cuando en realidad no están presentes. De este modo, una vez instalado el estereotipo del hacker como aquel que ingresa en sistemas informáticos violando las barreras de seguridad para producir daños o robar, toda acción anónima ocurrida en este sentido será atribuida a un hacker, reforzando simultáneamente el estereotipo.

Aún es mucho lo que resta por hacer en el trabajo de análisis. No hemos todavía analizado la macroestructura semántica. Los titulares por lo general coinciden con la macroproposición de primer nivel, expresando la idea central de la nota periodística, que es simultáneamente la que mejor se evoca, o incluso la única que se evoca pasados unos tres meses. Tampoco hemos analizado aun la superestructura de las noticias. No hemos profundizado lo suficiente en las cuestiones de estilo, retórica y argumentación. Queda pendiente además la exploración de los aspectos cognitivos del análisis, como las redes conceptuales y los modelos situacionales. Asimismo esperamos incorporar al corpus las noticias publicadas durante el corriente año en los mismos medios y realizar posteriormente una análisis comparativo con notas publicadas en otros medios especializados en temas de seguridad informática. Pensamos que nuestra comprensión de la construcción del estereotipo de hacker que realizan los medios puede verse aún muy enriquecida por el trabajo pendiente.

Bibliografía

Foucault, Michel (1991): La arqueología del saber. Ed.. Siglo XXI. 15º de., México.

Magariños de Morentín, Juan Angel (1993): La semiótica de enunciados. I.I.C.S., Investigación 10, U.N.L.P., La Plata.

Magariños de Morentín, Juan Angel (1996a): Los fundamentos lógicos de la semiótica y su práctica. Ed. EDICIAL, Bs. As.

van Dijk T. A. (1978): La ciencia del texto. Ed. Paidós. 3º ed., Barcelona.

van Dijk T. A. (1980): La noticia como discurso. Comprensión, estructura y producción de la información. Ed. Paidós, Barcelona.

van Dijk T. A. (1997): Racismo y análisis crítico de los medios. Ed. Paidós. Barcelona.

van Dijk T. A. (comp.)(2000): El discurso como interacción social. Ed. Gedisa, Barcelona.